Alcatel-Lucent 8950 AAA

Release 6.6.1

Enterprise Business Solution

User Guide

365-360-005
JUNE 2010
ISSUE 1.0

Legal notice

Alcatel, Lucent, Alcatel-Lucent, and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Copyright © 2010 Alcatel-Lucent. All rights reserved.

.

Contents

About this document **xiii**

Purpose ... xiii

Intended audience ... xiii

Supported systems ... xiii

How to use this document ... xiii

Conventions used ... xiv

Document support ... xiv

Technical support ... xiv

How to order ... xv

How to comment ... xv

Part I: 8950 AAA in enterprise solution **1**

1 Enterprise network with 8950 AAA **3**

Description ... 4

EBG architecture diagram ... 4

EBG components and roles ... 5

Access control process ... 6

Network interfaces ... 7

User profile stores ... 8

End devices in enterprises network ... 9

2 8950 AAA overview **11**

Description ... 12

Product features of 8950 AAA ... 12

Access restrictions ... 13

AAA redundancy ... 13

Authentication methods ... 13

Accounting status type ... 14

Components of 8950 AAA ... 15

8950 AAA component interfaces ... 17

Part II: 8950 AAA installation **19**

3 8950 AAA hardware and operating platform **21**

Operating platform and environment ... 21

Server memory ... 22

Server storage 22
Hardware requirements 22
4 Set up 8950 AAA for enterprise network 25
Set up 8950 AAA 25
5 Installation of 8950 AAA server and PolicyAssistant 27
Installation on Microsoft Windows 27
Install sample policies and rules for enterprise network 34
Start SMT on Windows platform 34
Part III: 8950 AAA PolicyAssistant 35
6 PolicyAssistant overview 37
PolicyAssistant 37
Start PolicyAssistant 38
Policy 38
Policy Wizard 39
7 Configure PolicyAssistant 41
Authentication methods 42
Configure policy selection rule 42
Configure PolicyAssistant rules for OmniSwitch 46
Configure EAP-MD5 authentication with Database as user source 46
Configure EAP-MD5 authentication with RADIUS User File as user source 54
Configure EAP-PEAP-MS-CHAPv2 authentication with RADIUS User File as user source 57
Configure EAP-PEAP-GTC authentication 62
Configure EAP-PEAP-AD authentication 66
Configure EAP-TLS authentication with RADIUS User File as user source 69
Configure EAP-TTLS-MS-Chapv2 authentication with RADIUS User File as user source 72
Configure authentication with Microsoft Active Directory as user source 75
Configure SAM authentication 78
Configure RSA/ACE server as a user source for secureID tokens 81
Configure proxy authentication for RADIUS server 84
Configure PolicyAssistant rules for CyberGateKeeper 87
Configure CG-pass-MD5 authentication with RADIUS User File as user source for Pass Audit 87
Configure CG-fail-MD5 authentication with RADIUS User File as user source for Fail Audit 90
Configure CG-NoAudit-MD5 authentication with RADIUS User File as user source for CG-NoAudit 92
Configure policy selection rules for CyberGateKeeper 94
Configure policy selection rule for CyberGateKeeper for Pass Audit 94
Configure policy selection rule for CyberGateKeeper for Fail Audit 96

Configure policy selection rule for CyberGateKeeper for Fail-NoAudit ... 97
8 Configure templates 101
Create a template ... 102
Edit a template ... 107
Delete a template ... 108
Part IV: 8950 AAA configuration 109
9 RADIUS client configuration 111
Any RADIUS client configuration ... 112
Identifying a client type ... 115
10 Vendor-specific attributes 117
Add vendor to the dictionary ... 118
Add vendor-specific attributes to the dictionary ... 119
11 8950 AAA policy server 123
8950 AAA policy server ... 123
Start policy server ... 124
From the SMT ... 124
From the command line window ... 125
As Windows service application ... 125
Configure 8950 AAA protocol properties for policy server ... 127
Configure delimiters for policy server ... 134
Configure timeout properties of policy server ... 136
12 8950 AAA Configuration server 139
8950 AAA configuration server ... 139
Configuration server properties ... 140
13 Derby database 143
Database configuration ... 143
Configure DB replication ... 146
Part V: 8950 AAA management 151
14 Remote configuration 153
8950 AAA remote configuration ... 153
Configure server entry ... 155
Add file list ... 158
Edit file list ... 163
Delete file entry ... 163
15 Certificate management 165
Certificates ... 165

Need for certificates 165
Encryption/Decryption using Digital certificates 166
Process to procure the digital certificate 167
Certificate deployment on 8950 AAA 168
Role of Certificate Manager 168
8950 AAA and certificates 168
Generate certificates for AAA using third-party CA 169

A Machine authentication 177

Glossary 183

List of figures

Figure 1-1 Architecture diagram of the EBG solution 5
Figure 1-2 Access Control Process 6
Figure 2-1 Components of 8950 AAA 15
Figure 2-2 Component interface diagram 17
Figure 5-1 Choose Destination Location 28
Figure 5-2 Choose Installation Type 29
Figure 5-3 License File Location 30
Figure 5-4 8950 AAA Administrator Configuration 31
Figure 5-5 8950 AAA Policy Set Installation 32
Figure 5-6 Certificate Configuration 33
Figure 6-1 PolicyAssistant 38
Figure 7-1 PolicyAssistant 43
Figure 7-2 Rule Configuration 44
Figure 7-3 Conditions 45
Figure 7-4 Simple panel 45
Figure 7-5 PolicyAssistant 46
Figure 7-6 Policy Configuration 47
Figure 7-7 Source for User Profiles 48
Figure 7-8 Authenticating Access Requests 49
Figure 7-9 Accounting Configuration 50
Figure 7-10 User and Session Limits 51
Figure 7-11 Database Configuration 52
Figure 7-12 Attribute Set for Policy 53
Figure 7-13 Policy configuration summary 54
Figure 7-14 User File Name Configuration 56
Figure 7-15 Policy configuration summary 57
Figure 7-16 Advanced Authentication Options 58
Figure 7-17 EAP PEAP Configuration 59
Figure 7-18 EAP MS CHAP V2 Authentication Configuration 60
Figure 7-19 CRL (Certificate Revocation List) Configuration 61
Figure 7-20 Policy configuration summary 62

Figure 7-21 Advanced Authentication Options 63
Figure 7-22 RSA ACE/Server Configuration 64
Figure 7-23 EAP GTC configuration 65
Figure 7-24 Policy configuration summary 66
Figure 7-25 Advanced Authentication Options 67
Figure 7-26 Policy configuration summary 69
Figure 7-27 TLS (Transport Level Security) Configuration 70
Figure 7-28 Policy configuration summary 71
Figure 7-29 Advanced Authentication Options 73
Figure 7-30 EAP TTLS Configuration 74
Figure 7-31 Policy configuration summary 75
Figure 7-32 Microsoft Active Directory Configuration 77
Figure 7-33 Policy configuration summary 78
Figure 7-34 Windows Security Access Manager 80
Figure 7-35 Policy configuration summary 81
Figure 7-36 RSA ACE/Server Configuration 82
Figure 7-37 Policy configuration summary 83
Figure 7-38 Radius Server (Proxy) Configuration 85
Figure 7-39 Policy configuration summary 86
Figure 7-40 Attribute Set for Policy 89
Figure 7-41 Policy configuration summary 90
Figure 7-42 Policy configuration summary 92
Figure 7-43 Policy configuration summary 94
Figure 7-44 Rule Configuration 95
Figure 7-45 Rule Configuration 96
Figure 7-46 Rule Configuration 98
Figure 8-1 User Files 102
Figure 8-2 User File List 103
Figure 8-3 User Files-users.templates 103
Figure 8-4 User Profile 104
Figure 8-5 Attribute Properties 105
Figure 8-6 User Profile for OmniSwitch 106
Figure 8-7 User Profile for CyberGateKeeper 106
Figure 9-1 Client Properties 112
Figure 9-2 Radius Client Properties 113
Figure 9-3 Client Classes and Attributes 116

Figure 10-1 Vendors 118
Figure 10-2 Vendor Name 119
Figure 10-3 Vendors - Attributes 119
Figure 10-4 Vendors - Attributes Properties 121
Figure 11-1 Windows Services 126
Figure 11-2 Windows Services 126
Figure 11-3 Radius Properties 128
Figure 11-4 Attributes Properties 131
Figure 11-5 Radius Request Properties 133
Figure 11-6 User Name Parsing Delimiters 135
Figure 11-7 Timeout Properties 137
Figure 12-1 Server Properties 140
Figure 13-1 Server Properties 144
Figure 13-2 Derby Databases 146
Figure 13-3 Derby Database Entry 147
Figure 14-1 8950 AAA remote configuration 155
Figure 14-2 Remote Configuration 156
Figure 14-3 Server Entry 157
Figure 14-4 File Selection Wizard 159
Figure 14-5 File Selection Wizard 160
Figure 14-6 File Selection Wizard – Selected file details 161
Figure 14-7 File Entry 162
Figure 15-1 Encryption and decryption with recipient keys 166
Figure 15-2 Encryption and decryption with sender keys 167
Figure 15-3 Digital Certificate 167
Figure 15-4 Deployment on 8950 AAA server 168
Figure 15-5 Microsoft Certificate Services 170
Figure 15-6 Request a Certificate 171
Figure 15-7 Advanced Certificate Request 172
Figure 15-8 Submit a Certificate Request or Renewal Request 173
Figure 15-9 Certificate Issued 174
Figure 15-10 Combining certificates 175
Figure 15-11 Local Security Settings 177
Figure 15-12 Access this computer from the network Properties 178
Figure 15-13 Select Users or Groups 178
Figure 15-14 Object Types 179

Figure 15-15 Select Users or Groups 179
Figure 15-16 Local Security Setting..... 180
Figure 15-17 Select Users or Groups 181
Figure 15-18 Act as part of the operating system properties..... 182

List of tables

Table 1-1 Supplicant types 9
Table 2-1 8950 AAA component interface 18
Table 9-1 RADIUS client Properties 113
Table 10-1 Vendor attributes 121
Table 11-1 RADIUS Properties 128
Table 11-2 TACACS+ Properties 131
Table 11-3 Attributes Properties 132
Table 11-4 RADIUS Requests Properties 133
Table 11-5 User Name Parsing Delimiters 135
Table 11-6 Timeout Properties 137
Table 12-1 Configuration Server properties 141
Table 13-1 Database Configuration 144
Table 13-2 Derby Database Entry 147
Table 13-3 Database Properties 148
Table 14-1 Server Entry 157
Table 14-2 File Entry 162

About this document

Purpose

This document describes the 8950 AAA server and its role in providing security to the enterprise business network. It provides procedures to configure the 8950 AAA server so that it interfaces with other network elements in the enterprise network, and provides security for the end user to access the network. It provides related procedures to configure the various components in the EBG network.

Intended audience

This document is intended for installation, operation, engineering and validation personnel, and other users in the capacity of network administrators familiar with 8950 AAA solutions.

Supported systems

This document applies to the System Release 8950 AAA Enterprise Business Group Solution 6.6.1.

How to use this document

The following table describes how to use this document:

Document organization	When to use
8950 AAA in enterprise solution	This part provides an overview of the enterprise business solution that offers integrated solutions in the AAA scenario that requires user-centric security.
8950 AAA installation	This part provides hardware and software information about the 8950 AAA server, and procedures to install the 8950 AAA in the enterprise network scenario on both Windows® and UNIX® platforms.
8950 AAA PolicyAssistant	This part describes the PolicyAssistant and the usage of the PolicyAssistant to configure the rules to provide network access to an enterprise user.

Document organization	When to use
8950 AAA configuration	This part describes the procedures to configure the 8950 AAA so that it interacts with various network elements in the enterprise network.
8950 AAA management	This part provides a description of tools and interfaces used in the management of 8950 AAA server.

Conventions used

This guide uses the following typographical conventions:

Appearance	Description
emphasis	Text that is emphasized
document titles	Titles of books or other documents
file or directory names	The names of files or directories
graphical user interface text	Text that is displayed in a graphical user interface
keyboard keys	The name of a key on the keyboard
`system input`	Text that the user types as input to a system
`system output`	Text that a system displays or prints
`variable`	A value or command-line parameter that the user provides
[ ]	Text or a value that is optional
{***`value1`*** | ***`value2`***} {***`variable1`*** | ***`variable2`***}	A choice of values or variables from which one value or variable is used

Document support

For support in using this document or any other Alcatel-Lucent document, contact Alcatel-Lucent at one of the following telephone numbers:

- 1-888-582-3688 (for the United States)
- 1-317-377-8618 (for all other countries)

Technical support

For technical support, contact your local Alcatel-Lucent customer support team. See the Alcatel-Lucent Support web site (http://alcatel-lucent.com/support/) for contact information.

How to order

To order Alcatel-Lucent documents, contact your local sales representative or use the Online Customer Support Site (OLCS) web site (http://support.alcatel-lucent.com/).

How to comment

To comment on this document, go to the Online Comment Form (http://infodoc.alcatel-lucent.com/comments/) or e-mail your comments to the Comments Hotline (mailto:comments@alcatel-lucent.com).

Part I: 8950 AAA in enterprise solution

Overview

Purpose

This part provides an overview of the enterprise network. The network offers integrated solutions along with the 8950 AAA server to provide user-centric security.

Contents

This part covers the following chapters.

Enterprise network with 8950 AAA	3
8950 AAA overview	11

1 Enterprise network with 8950 AAA

Overview

Purpose

This chapter provides an overview of the enterprise network. It describes the various components and interfaces in the enterprise network and their roles. It also explains the role of the 8950 AAA server in providing user-centric security in the enterprise network.

Contents

This chapter covers the following topics.

Description	4
EBG architecture diagram	4
EBG components and roles	5
Access control process	6
Network interfaces	7
User profile stores	8
End devices in enterprises network	9

Description

The enterprise business solution is an integrated security solution implemented in an enterprise network. The integrated solution uses the 8950 AAA server in providing user-centric security to the enterprise network. The user-centric security blueprint prescribes a global, corporate-wide security infrastructure. Simultaneously, it separates the responsibility of providing security from the endpoints and applications. It also assists in developing an independent chain of control for security, and protects the endpoints. Additionally, it provides an always-on and highly available security that is transparent to the end user.

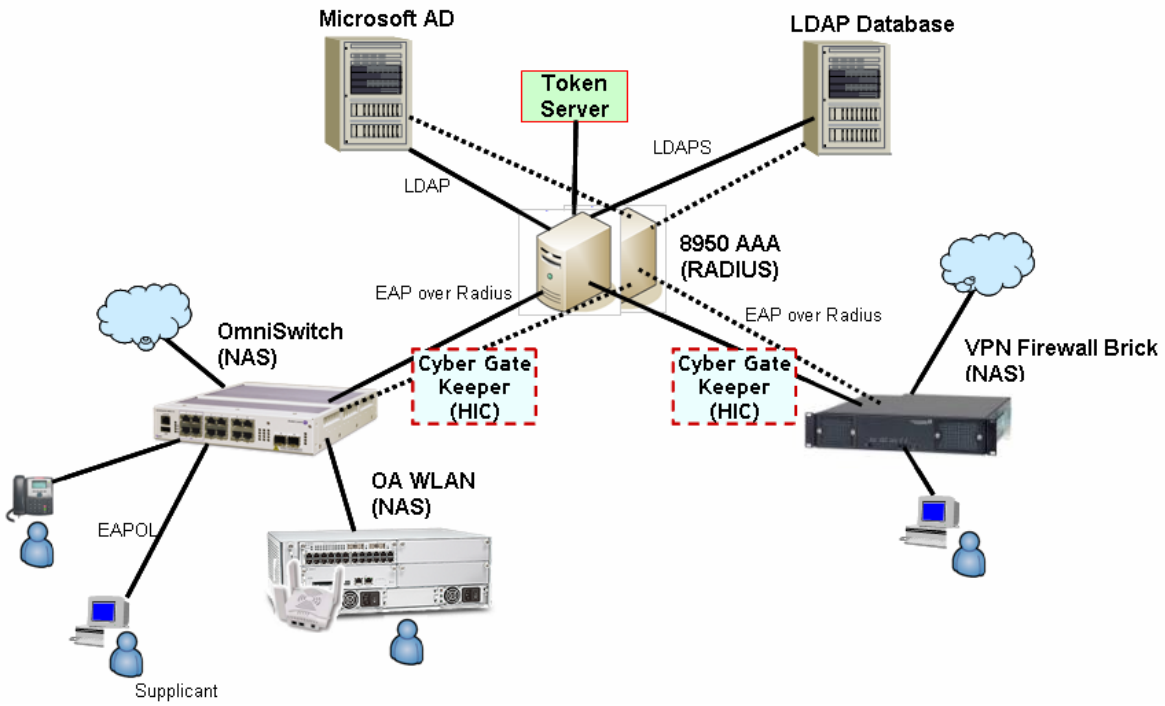
The security architecture encompasses all the security modules in the network, such as the IP firewall, the VPN, and the components that perform threat management. The security architecture utilizes the authenticated identity of the end device (user credentials, device credentials, or both) and protects the content of all messages in the network. This also allows the network administrator to control the user access to the network resources and applications.

The 8950 AAA server provides a full-featured RADIUS protocol based solution to support the requirements of the core identity management, that is, the access and authorization process in the enterprise solutions.

EBG architecture diagram

Figure 1-1 depicts the overall architecture of the enterprise network. The 8950 AAA server provides authentication, authorization, and accounting services to users or devices connected to the edge network elements. The figure illustrates how the end users are connected to the edge devices in the enterprise network. OmniSwitch, Brick Firewall, and OmniAccess WLAN are the edge devices in the Alcatel-Lucent enterprise network. CyberGateKeeper provides the auditing of host configuration and is placed behind the OmniSwitch. This element is optional in an enterprise network. In scenarios that do not have CyberGateKeeper, the RADIUS clients or the edge devices such as the OmniSwitch directly interface with the 8950 AAA. User profile stores like LDAP server, database server, Windows AD server are behind the 8950 AAA server. The 8950 AAA server uses the user profile stores to authenticate and authorize the users or devices that connect to the enterprise network.

Figure 1-1 Architecture diagram of the EBG solution



EBG components and roles

This topic provides a list of components in the enterprise network solution, and briefly describes their roles and functions.

8950 AAA Server (RADIUS): The 8950 AAA provides authentication, authorization, and accounting services for wired, wireless, and converged networks. The 8950 AAA supports RADIUS protocol for authentication services. In an enterprise network, the 8950 AAA supports multiple 802.1x port authentication using EAP framework. In addition, the 8950 AAA interfaces with external LDAP servers, Windows Active Directory®, JDBC database, and others to authenticate and authorize enterprise endpoints. These external servers store authentication details about users, user groups, NAS devices, and so on. The 8950 AAA server provides the following functionality:

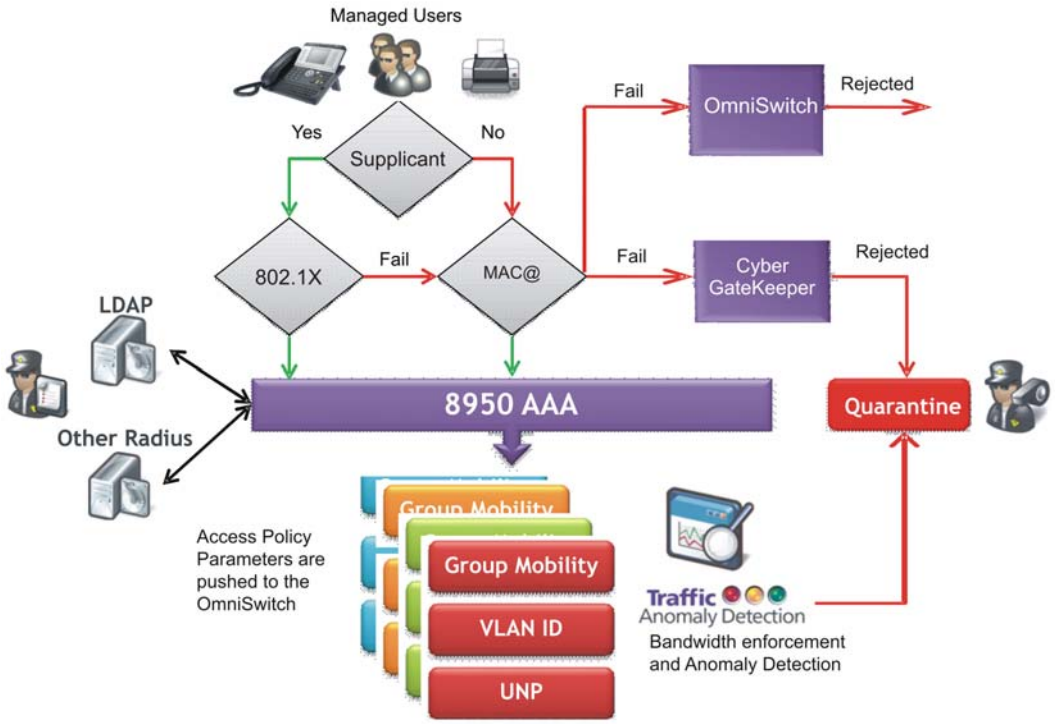
a. Extensive AAA protocol support
b. Remote configuration management
c. Comprehensive monitoring and reporting

Network Access Server (NAS): The Network Access Server (NAS) is the client-gateway to access the network resources. The NAS supports RADIUS, 802.1x, and EAP protocols for communicating with the 8950 AAA server to provide access to the users. In an enterprise network, the client network elements that communicate with the 8950 AAA server are OmniSwitch, VPN Brick firewall, Omni Access, and Omni Access WLAN.

Supplicants: Supplicants are the end-user devices that connect to the NAS, for example, a computer, a laptop, a PDA, a Smartphone, and so on. The supplicant can also be the resident software on client devices. This software allows the end-user devices to connect to the NAS over the 802.1x protocol.

Access control process

Figure 1-2 Access Control Process



The following steps describe the user access-control process in the enterprise network.

1 The 8950 AAA authenticates users based on user and device credentials, or only user credentials as part of the 802.1x authentication. In other scenarios like IP Touch phone, only device credentials are verified through MAC address authentication.

If...	then...
the end-user device is a recognized supplicant	the end user is authenticated through 802.1x authentication protocol.
the end-user device is an unrecognized supplicant	the end user is authenticated through MAC address authentication protocol.

2 The 8950 AAA server authenticates the user credentials by checking against the built-in Derby database, LDAP servers or other external databases like Windows AD.

3 The 8950 AAA server authorizes the user to access the services, and starts the accounting process.

4 If the 8950 AAA server fails to recognize and authenticate a user, the next action depends upon the presence of the CyberGateKeeper in the enterprise network.

If...	then...
CyberGateKeeper is present	the CyberGateKeeper performs a host integrity check and the user is quarantined for further administrative investigations.
CyberGateKeeper is not present	the RADIUS client rejects the user and denies access of services to the user.

Network interfaces

This topic provides a list of the network elements that the 8950 AAA interface with in an enterprise network, and provides a brief description of each of them.

OmniSwitch

The OmniSwitch is an advanced fixed configuration family of Ethernet switches. These switches provide wire rate Layer 2 forwarding and Layer 3 routing with advanced services.

They are fixed configuration, triple-speed (10/100/1000) switches that provide the following features:

- Increased network performance
- Improved application response times
- Secured LAN
- Enhanced user productivity by maximizing mobility, network capacity, and services over existing category

CyberGateKeeper

The CyberGateKeeper is positioned between the NAS and the 8950 AAA RADIUS server. It audits all networked systems continuously for policy compliance. Unqualified systems attempting to access the network are quarantined by this network element and redirected for remediation.

The CyberGateKeeper provides the following functionalities:

- Achieves comprehensive policy compliance
- Assists in antivirus and software updates
- Continuously audits network systems
- Fully scalable
- Supports centralized management and custom tests
- Allows efficient remediation

Brick firewall

The Brick provides high-speed firewall, VPN, QoS, VLAN, and virtual firewall capabilities in a single configuration. The functionalities of the Brick also include advanced distributed denial of service attack protection, strong authentication, real-time monitoring, logging, and reporting.

Omni Access WLAN

OmniAccess WLAN is a wireless access point through which mobile users connect to the enterprise network. The 8950 AAA server authenticates and authorizes the users or supplicants as they scan and connect to wireless access points.

User profile stores

This topic provides a list of internal and external user profile stores (subscriber databases) used in the enterprise. Figure 1-1 provides an overview of the enterprise network.

Customers with a smaller user base can use the built-in Derby database. For a large user base customers can choose external databases to store user details like user logins, passwords, authorization profiles, and so on.

Database

8950 AAA supports external databases like Oracle, MySQL, MS SQL server, which support JDBC.

The following information is stored in databases:

- Home subscribers authentication information
- User information
- Profiles for verification
- Profile to return to the access controllers (authorization data)

LDAP

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying data using directory services running over TCP/IP. The 8950 AAA server supports the following LDAP databases:

- Sun One DS
- OpenLDAP
- 8661 DS

Microsoft AD

The 8950 AAA authenticates Windows users and machines user profiles stored in Microsoft® AD.

Files

8950 AAA can authenticate user profiles from flat file database.

End devices in enterprises network

The 8950 AAA server can authenticate the following end user devices in an enterprise network:

- Dual-mode WiFi Smartphones
- Corporate computer
- Home computer
- Public computer

For more information on the device or supplicant types, see Table 1-1.

Supplicant types

Table 1-1 depicts the supplicant types supported by the 8950 AAA.

Table 1-1 Supplicant types

Supplicant	Web site	Product type	Comments
Windows XP Supplicant	http://www.microsoft.com/en/us/default.aspx	Commercial (included in Windows XP)	Included in Windows XP
Juniper Odyssey	http://www.juniper.net/customers/support/products/oac.jsp	Commercial	Available for XP and Windows 7

The 8950 AAA can possibly support other combinations that are not tested.

2 8950 AAA overview

Overview

Purpose

This chapter describes the features, functions, and supported protocols of 8950 AAA server that are available in the enterprise network.

Contents

This chapter covers the following topics.

Description	12
Product features of 8950 AAA	12
Access restrictions	13
AAA redundancy	13
Authentication methods	13
Accounting status type	14
Components of 8950 AAA	15
8950 AAA component interfaces	17

Description

The 8950 AAA server is a network entity that provides authentication, authorization, and accounting functionalities in carrier and enterprise networks. In an enterprise network, the 8950 AAA server interfaces with 802.1x switches, wireless access points, and audit solutions like CyberGateKeeper. The 8950 AAA server supports RADIUS protocol to interface with the edge devices.

Product features of 8950 AAA

The following list describes a few features of 8950 AAA relevant to an enterprise network:

- 8950 AAA supports the 802.1x authentication using the following EAP protocols:
  - EAP-TLS
  - EAP-TTLS
  - EAP-PEAP
  - EAP-MD5
  - EAP-GTC
- 8950 AAA implements XML-based dictionary which is a superset of RFC standard and Vendor Specific Attributes (VSA). This design provides the 8950 AAA, the ability to adapt to various vendors of edge devices in an enterprise network.
- 8950 AAA offers a built-in programming language for writing custom AAA policy applications. This powerful PolicyFlow™ language allows configuring the 8950 AAA according to any complex policy rules of an enterprise. PolicyFlow architecture built on Java™ programming language is flexible and extensible.
- *PolicyAssistant* is a graphical wizard to define policies for enterprise policy rules. If the application requires complex policies, use policy flows instead of the PolicyAssistant.
- Logging mechanism is flexible and configured according to the requirements.
- The Server Management Tool (SMT) provides a graphical remote configuration and management interface to all of the 8950 AAA features.
- In addition to the SMT, the 8950 AAA provides a Command Line Interface (CLI), which allows you to access and operate the 8950 AAA in the enterprise network environment. It supports Telnet and SSH-based CLI through the admin console. An administrator can use this CLI for executing commands for administrative purposes.

Access restrictions

With the help of 8950 AAA, the user can define authorization rules and decide on the type of access provided to the user after successful authentication.

For example, the access restrictions imposed can depend on the role of the user and they are defined by the user profiles in the Microsoft AD. 8950 AAA retrieves the Local-Groups or the Global-Groups fields during authentication through the Microsoft AD. These groups are verified against the rules of the enterprise and the appropriate access is provided.

For example, an employee in the accounts domain is allowed to access the corporate network internally (OmniSwitch using 802.1x), while a sales employee is allowed to access the network using the VPN, Corporate LAN, or corporate WiFi network.

AAA redundancy

You can configure the 8950 AAA server on two machines to support redundancy. You can configure the two servers in the following two modes:

1. **Active – Active**: In this mode, both servers share the load. In case one server fails, the active server takes over. The load-sharing mode resumes, once the failed server is restored.
2. **Active – Standby**: In this mode, one server is always on standby mode to take over when the active server fails.

Authentication methods

The authentication mechanisms supported for an enterprise network are as follows:

Device only authentication

MAC address authentication – Authenticates the MAC address of the device against the device details in a flat file or database. Example, IP touch phone is one of the devices that gets authenticated with this method.

Authentication using certificates – End device and the server could mutually authenticate each other using X.509 certificates. EAP-TLS is the protocol is that is used to support this authentication mechanism.

User Only authentication

In this scenario, only user name and password are authenticated. EAP-MD5, EAP-GTC with RSA ACE are the protocols that are used to support this authentication mechanism.

Authentication using certificates along with user authentication

In this scenario, user credentials as well as the certificates installed on the server and device are authenticated. EAP-TTLS, EAP-PEAP are the protocols that are used to support this authentication mechanism.

Accounting status type

The 8950 AAA supports RADIUS accounting protocol as defined by RFC 2866. This protocol carries accounting information between NAS and a shared accounting server. Following are the various accounting records sent by the RADIUS client to the 8950 AAA server:

Start

At the start of the service delivery, the client configured to use RADIUS Accounting services, generates an Accounting Start packet describing the user and type of service delivered.

Stop

At the end of the service delivery, the client generates an Accounting Stop packet describing the type of service delivered and optional statistics such as elapsed time, input and output octets, or input and output packets.

Accounting-On

This marks the start of accounting (for example, upon booting) by specifying the attribute as *Accounting-On.*

Accounting-Off

This marks the end of accounting (for example, just before a scheduled reboot) by specifying the attribute as *Accounting-Off.*

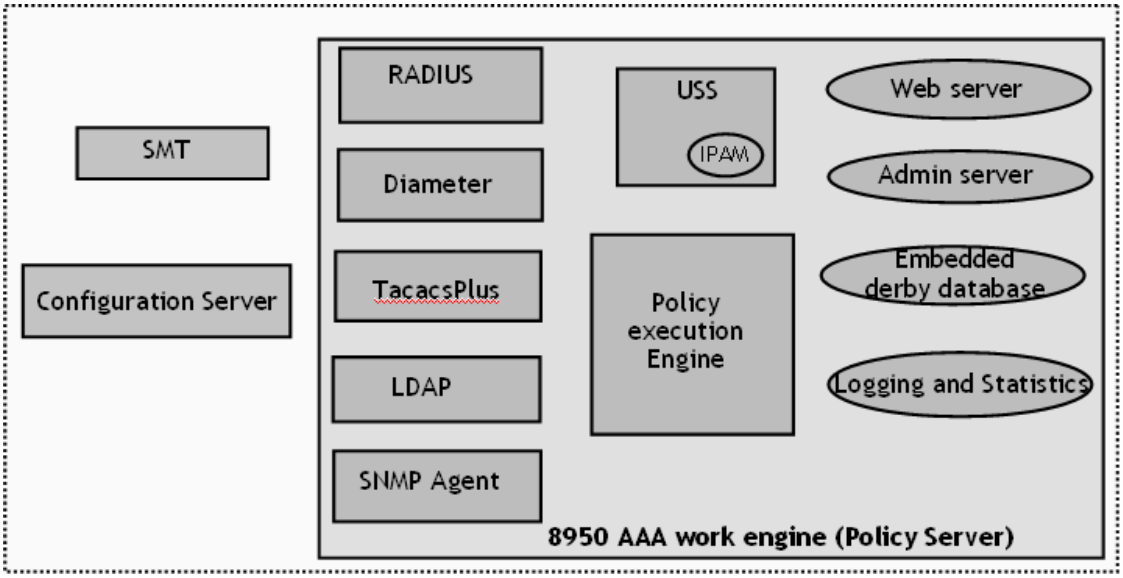
Interim-update

Interim accounting is a periodical update from the RADIUS client (NAS) to the 8950 AAA accounting server sent after the accounting *Start* and before accounting *Stop.* These records indicate that the session is active and provide the network usage details, such as time elapsed since session started, packets sent over the wire until now, and so on to the accounting server.

Components of 8950 AAA

This topic provides a list of components of the 8950 AAA server and a brief explanation of all these components. Figure 2-1 illustrates different components of 8950 AAA.

Figure 2-1 Components of 8950 AAA



RADIUS

RADIUS listener of 8950 AAA handles the RADIUS requests sent by 8950 AAA clients.

TacacsPlus

TacacsPlus listener of 8950 AAA handles the TacacsPlus requests sent by 8950 AAA clients.

Embedded Derby database

Derby is an embedded database, which stores the user profiles for 8950 AAA. Customers with a smaller subscriber database can use the built-in Derby database.

LDAP

8950 AAA has an LDAP listener for handling LDAP requests. Policy flow processes these requests. Supported LDAP operations are Bind, Search, Compare, Add, Modify, and Delete.

Server Management Tool (SMT)

Server Management Tool (SMT) is the graphical user interface to 8950 AAA. SMT provides access to different components of 8950 AAA. SMT is used to administer the product.

Admin server

The admin server allows you to interact with 8950 AAA independent of the SMT. You can connect to the Admin server using Telnet and SSH console. The 8950 AAA supports CLI for remote login and debugging purposes. Administrator can use this CLI for executing commands for administrative purposes.

Configuration server

Configuration server allows administrators to access remote 8950 AAA server by using the SMT.

Web server

The 8950 AAA server has a built-in web server for performing the following functions:

- Display server information, such as version of 8950 AAA, host name, java version, and so on.
- Track authentication and accounting statistics.
- Maintain the 8950 AAA documentation index, to provide all information related to 8950 AAA product.
- Maintain User Provisioning Tool (UPS), to provision user profiles in Derby database.

Universal State Server (USS)

Universal State Server (USS) of 8950 AAA is an in-memory database, held in RAM. USS has a centralized view of the active AAA sessions.

Policy execution engine

Policy execution engine of 8950 AAA processes the requests of RADIUS. Policy engine works with the PolicyFlow language and uses PolicyFlow plug-ins at run time to process the requests. This plug-in architecture with sophisticated logic programming capabilities provides unlimited flexibility. It allows you to define and implement AAA access policies, without custom software development. 8950 AAA policy engine is built around a robust core request queue processor. The processor receives incoming requests and routes them through selected processing plug-in functions. The request queue performs duplicate request detection and automatic deletion of *timed-out* requests. This optimization avoids the time spent on processing stale or duplicate requests and increases actual throughput over other AAA servers, with similar transaction ratings.

SNMP agent

8950 AAA offers statistical information through SNMP. The SNMP agent of 8950 AAA interacts with the SNMP manager to view the statistical data for every client as well as aggregate statistics. 8950 SNMP agent supports only read only operation.

Logging and statistics

The logging component of 8950 AAA creates and writes log messages for all the server actions. 8950 AAA allows you to view the server-related statistics and the status of requests sent and received by 8950 AAA server.

8950 AAA component interfaces

Figure 2-2 illustrates the components interface diagram.

Figure 2-2 Component interface diagram

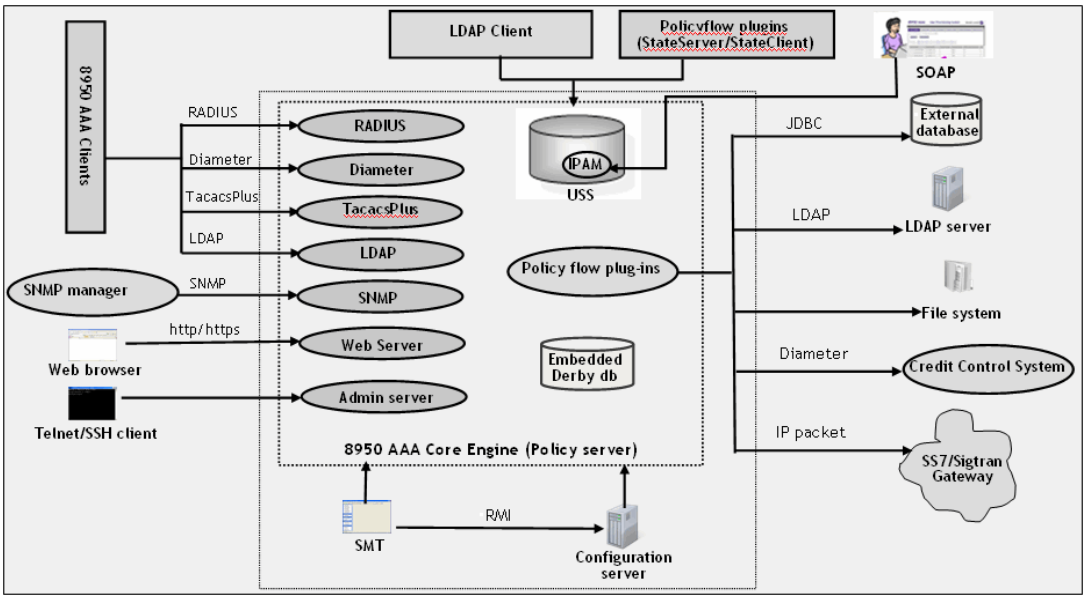


Table 2-1 describes the different components of 8950 AAA and the clients.

Table 2-1 8950 AAA component interface

8950 AAA component	Client	Description
8950 AAA	8950 AAA clients	8950 AAA interacts with clients such as NAS, B-RAS, HA, LDAP client, WAC, and proxy AAA using 8950 AAA components such as RADIUS, Diameter, TacacsPlus, and LDAP.
SNMP agent	SNMP manager	8950 AAA interacts with SNMP manager using SNMP agent.
Web server	Web browser	8950 AAA has a built-in web server for handling http requests. This server also hosts SOAP web services.
Admin server	Telnet/SSH	Admin server component enables you to interact with 8950 AAA using admin interface commands. Admin server can be connected using Telnet and SSH consoles.
USS	LDAP client	USS offers an LDAP interface to enable the external elements to view or search information of current sessions.
USS	PolicyFlow plug-ins	Access USS using PolicyFlow plug-ins such as StateServer and StateClient. PolicyFlow plug-in allows you to edit and delete the session information.
PolicyFlow Plug-ins	External systems	JDBC, LDAP, and Diameter plug-ins are used to access external database (SQL), LDAP server, and credit control system respectively.

Part II: 8950 AAA installation

Overview

Purpose

This part provides hardware and software information about the 8950 AAA server, and procedures to install the 8950 AAA in the enterprise network scenario.

Contents

This part covers the following chapters.

8950 AAA hardware and operating platform	21
Set up 8950 AAA for enterprise network	25
Installation of 8950 AAA server and PolicyAssistant	27

3 8950 AAA hardware and operating platform

Overview

Purpose

This chapter provides hardware and operating platform requirements for the 8950 AAA server.

Contents

This chapter covers the following topics.

Operating platform and environment	21
Server memory	22
Server storage	22
Hardware requirements	22

Operating platform and environment

8950 AAA supports Microsoft Windows 2003, Windows XP, and Windows Server 2008 platforms.

8950 AAA requires Java 2 Standard Edition (J2SE) version 6.x or later to run on all platforms. Both J2SE JDK and JRE are supported. However, JDK is recommended as it provides additional tools for supporting Java applications.

Contact the operating system vendor or http://java.sun.com/ for information on Java support for your computer. Ensure that the Java environment maintains the current patch levels.

Server memory

By default, memory allocated for 8950AAA process is 512 MB for a 32-bit JVM.

The memory usage depends on a number of factors, few of which are listed as follows:

- Server configuration
- User file size (when used)
- Total number of active subscribers (during peak hour)
- Platform – check whether the USS and the SMT runs on the same platform as the 8950 AAA server

Note: For memory configuration, contact 8950 AAA support team to get a confirmation on:

a. Use of JVM 32 bit or 64 bit

b. Memory allocated for each type of JVM

Server storage

The server must have at least 100 MB of free disk space for installation.

Note: The storage requirement of 100 MB is for installation. For daily operations, allow extra storage space for accounting data and log files. The actual amount of disk space needed for logs and accounting records depends on many factors such as logging level, accounting detail, and the length of time for which the data is retained.

Hardware requirements

The performance of the 8950 AAA software depends on a variety of factors that are listed as follows.

- Peak usage and average session times expected.
- Storage of subscriber information, such as SQL Database (Oracle or Sybase) or an LDAP directory (Sun One Directory).
- Hardware currently used, such as Sun Servers or Intel Based server (number of CPUs, Memory).
- Number of subscribers or the number of ports used in the system.
- Type of connection services that are available, such as dial-in, DSL, VPN, 802.11 Wireless LAN (802.1x), or 3G-1X Data.
- Operating system that the customer prefers, such as Windows, Intel, and Linux.

- Layout of the physical network, such as the location of RADIUS clients.

Contact Alcatel-Lucent support channel to determine the hardware necessary to run the 8950 AAA server in your production environment.

4 Set up 8950 AAA for enterprise network

Overview

Purpose

This chapter provides a sequential approach to commission the 8950 AAA server in the enterprise network. The procedure provides links to chapters that contain detailed procedures for each task.

Contents

This chapter covers the following topics.

Set up 8950 AAA	25

Set up 8950 AAA

Follow these steps to install, configure, and manage 8950 AAA in an enterprise network.

1 Install the 8950 AAA server.

For more details on installation of the 8950 AAA server, see Chapter 5, Installation of 8950 AAA server and PolicyAssistant.

2 Copy 8950 AAA sample policies and rules for enterprise network.

For more details, see procedure, Install sample policies and rules for enterprise network.

3 Configure the policy rules or policies according to the requirements of the enterprise network.

For sample configurations of policies and rules, see Chapter 7, Configure PolicyAssistant.

4 Perform general configuration procedures on the 8950 AAA server.

For detailed procedures, see Part 4, 8950 AAA configuration.

5 For details on 8950 AAA server management, see Part 5, 8950 AAA management.

5 Installation of 8950 AAA server and PolicyAssistant

Overview

Purpose

The key feature in an enterprise network is the PolicyAssistant. You can configure the PolicyAssistant according to the requirements in the enterprise network. This chapter describes the procedures to install 8950 AAA, PolicyAssistant, and sample enterprise policy rules. Modify the sample rules according to the enterprise requirements.

Contents

This chapter covers the following topics.

Installation on Microsoft Windows	27
Install sample policies and rules for enterprise network	34
Start SMT on Windows platform	34

Installation on Microsoft Windows

Purpose

Use this procedure to install 8950 AAA PolicyAssistant on Microsoft Windows.

Before you begin

Ensure that you have a valid license file for the 8950 AAA software version you need to install.

Procedure

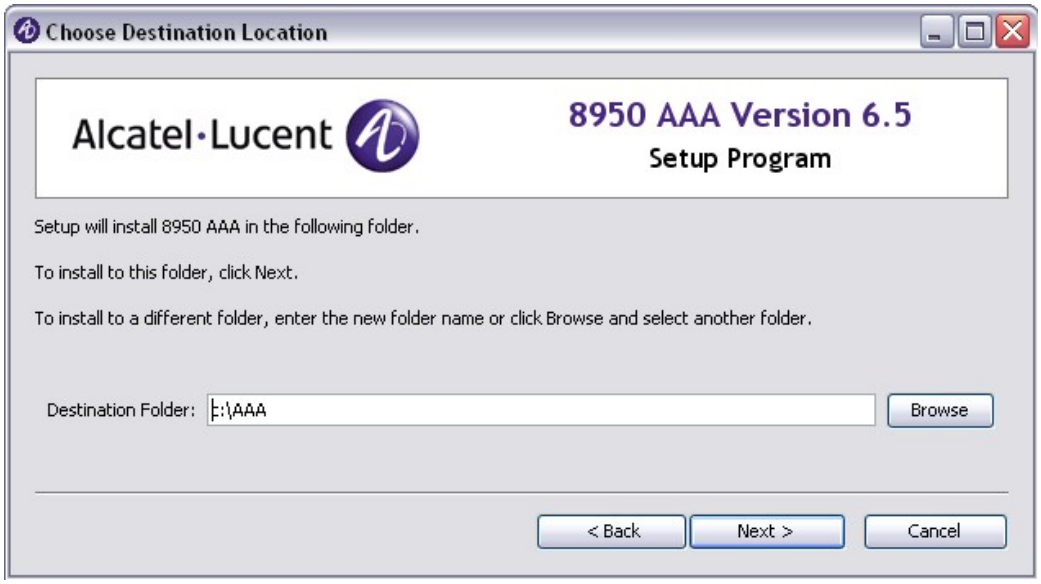
1. Double-click *8950 aaa-6.x .zip* and extract the files to a temporary directory.
2. Navigate to the location of the unzipped 8950 AAA files and double-click *setup.exe*. The 8950 AAA Setup program appears.

   Result: Click **Next**. The **Software License Agreement** window opens.

3. Accept the license agreement terms and click **Next**.

   Result: The **Choose Destination Location** window opens.

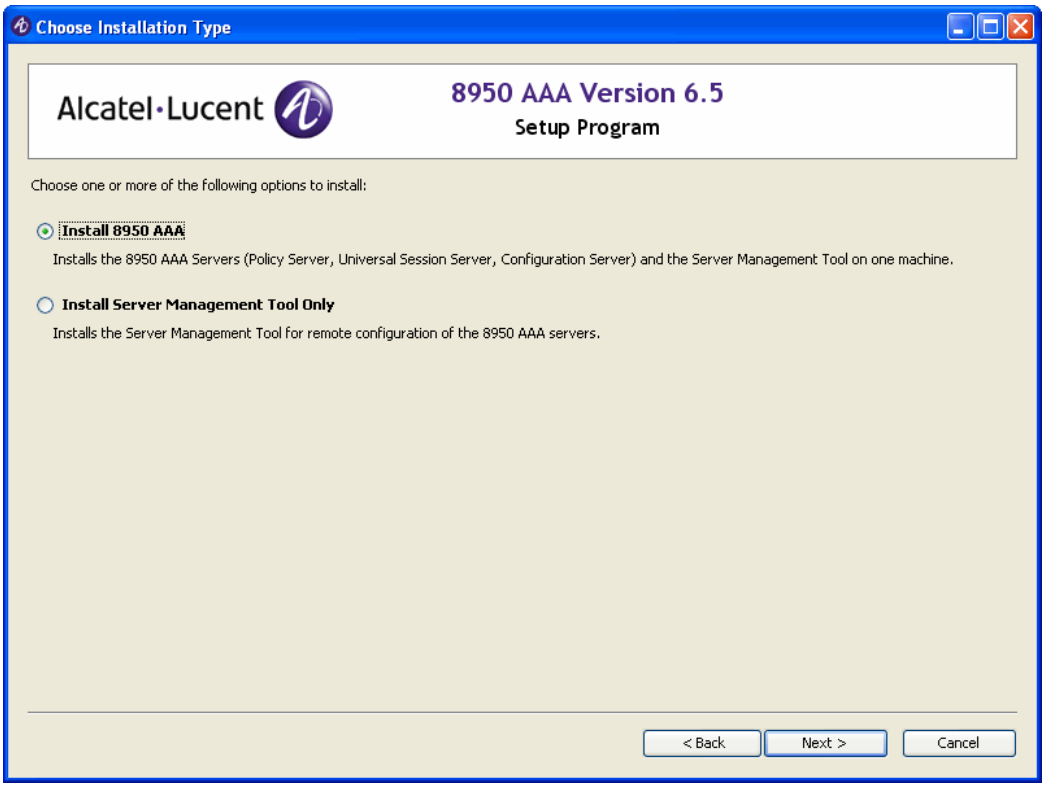
Figure 5-1 Choose Destination Location


Choose Destination Location
Alcatel·Lucent
8950 AAA Version 6.5
Setup Program
Setup will install 8950 AAA in the following folder.
To install to this folder, click Next.
To install to a different folder, enter the new folder name or click Browse and select another folder.
Destination Folder:
E:\AAA
Browse
< Back
Next >
Cancel

4. To use the default installation location, click **Next**. To choose a different location, click **Browse** and select the desired location.

   Result: The **Choose Installation Type** window opens.

Figure 5-2 Choose Installation Type


Choose Installation Type
Alcatel·Lucent
8950 AAA Version 6.5
Setup Program
Choose one or more of the following options to install:
Install 8950 AAA
Installs the 8950 AAA Servers (Policy Server, Universal Session Server, Configuration Server) and the Server Management Tool on one machine.
Install Server Management Tool Only
Installs the Server Management Tool for remote configuration of the 8950 AAA servers.
< Back
Next >
Cancel

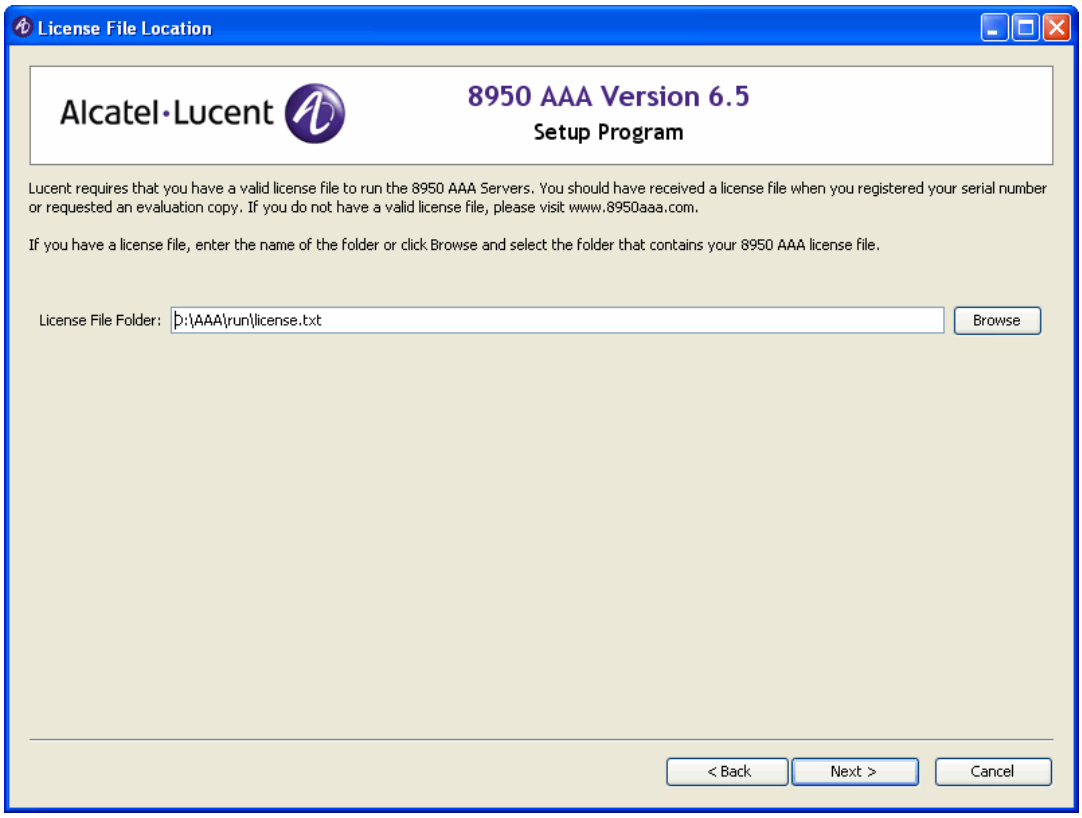
5 Select the required installation type from the following and click **Next.**

a. Select **Install 8950 AAA** option to install both 8950 AAA server and the SMT GUI client application.

b. Select **Install Server Management Tool Only** option to install only the SMT GUI application to manage and monitor a remote 8950 AAA server.

Result: The **License File Location** window opens.

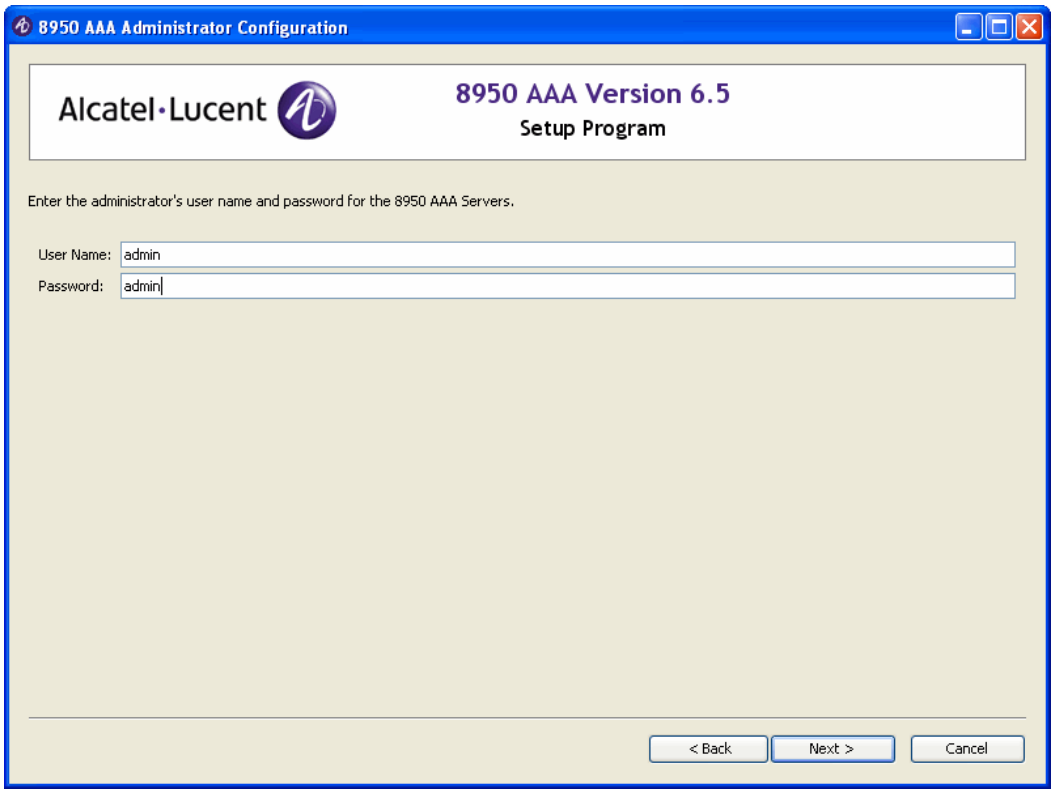
Figure 5-3 License File Location


License File Location
Alcatel·Lucent
8950 AAA Version 6.5
Setup Program
Lucent requires that you have a valid license file to run the 8950 AAA Servers. You should have received a license file when you registered your serial number or requested an evaluation copy. If you do not have a valid license file, please visit www.8950aaa.com.
If you have a license file, enter the name of the folder or click Browse and select the folder that contains your 8950 AAA license file.
License File Folder:
D:\AAA\run\license.txt
Browse
< Back
Next >
Cancel

6 Enter the name of the folder or click **Browse** to specify the location of the license file, and click **Next**.

Result: The **8950 AAA Administrator Configuration** window opens.

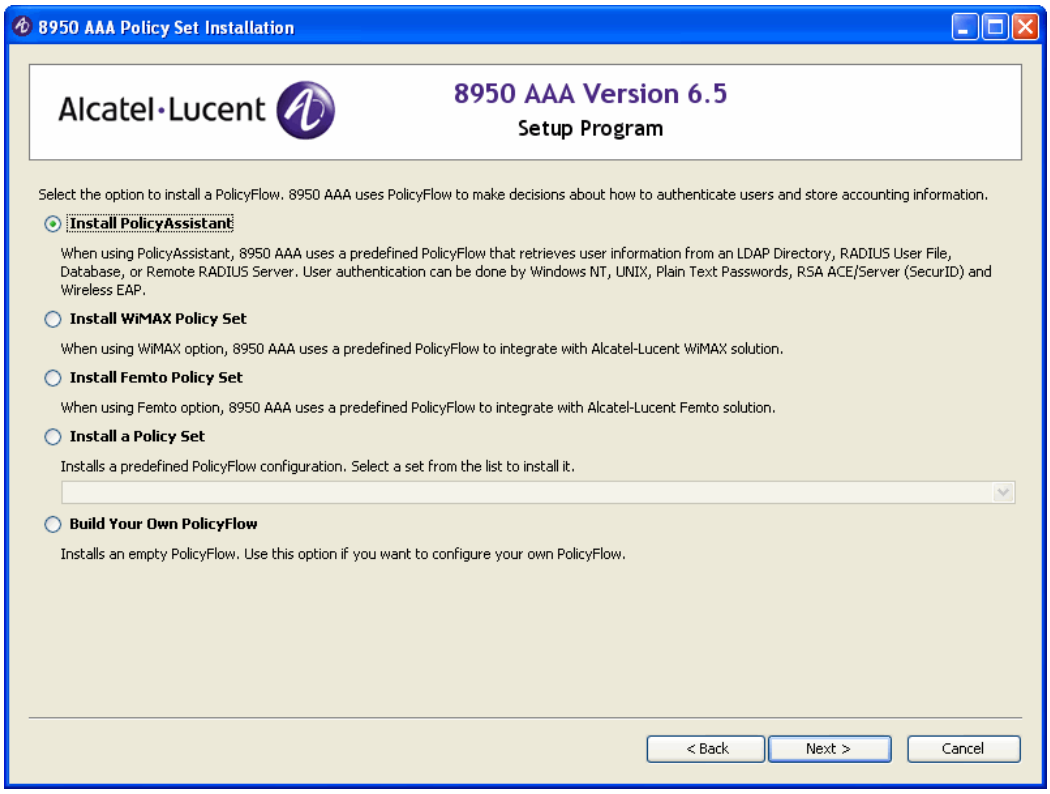
Figure 5-4 8950 AAA Administrator Configuration



7 Enter the administrator username and password and click **Next**.

Result: The **8950 AAA Policy Set Installation** window opens.

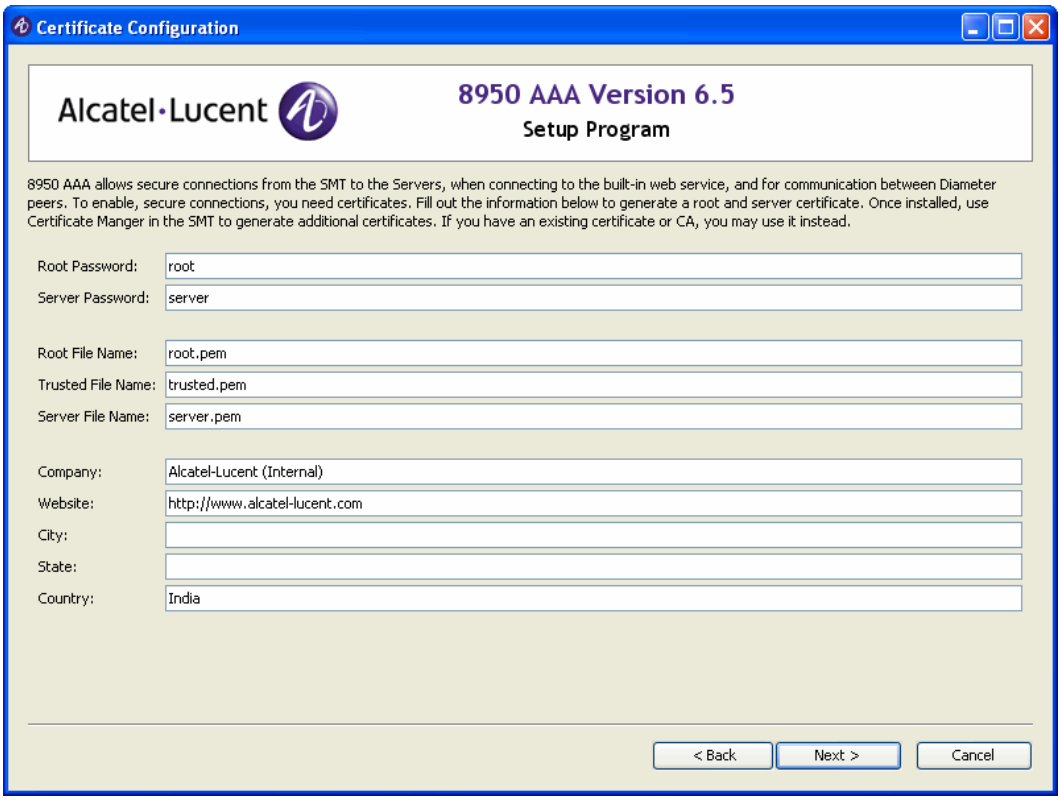
Figure 5-5 8950 AAA Policy Set Installation


8950 AAA Policy Set Installation
Alcatel·Lucent
8950 AAA Version 6.5
Setup Program
Select the option to install a PolicyFlow. 8950 AAA uses PolicyFlow to make decisions about how to authenticate users and store accounting information.
Install PolicyAssistant
When using PolicyAssistant, 8950 AAA uses a predefined PolicyFlow that retrieves user information from an LDAP Directory, RADIUS User File, Database, or Remote RADIUS Server. User authentication can be done by Windows NT, UNIX, Plain Text Passwords, RSA ACE/Server (SecurID) and Wireless EAP.
Install WiMAX Policy Set
When using WiMAX option, 8950 AAA uses a predefined PolicyFlow to integrate with Alcatel-Lucent WiMAX solution.
Install Femto Policy Set
When using Femto option, 8950 AAA uses a predefined PolicyFlow to integrate with Alcatel-Lucent Femto solution.
Install a Policy Set
Installs a predefined PolicyFlow configuration. Select a set from the list to install it.
Build Your Own PolicyFlow
Installs an empty PolicyFlow. Use this option if you want to configure your own PolicyFlow.
< Back
Next >
Cancel

8 Select **Install PolicyAssistant** and click **Next**.

Result: The **Certificate Configuration** window opens.

Figure 5-6 Certificate Configuration


Certificate Configuration
Alcatel·Lucent
8950 AAA Version 6.5
Setup Program
8950 AAA allows secure connections from the SMT to the Servers, when connecting to the built-in web service, and for communication between Diameter peers. To enable, secure connections, you need certificates. Fill out the information below to generate a root and server certificate. Once installed, use Certificate Manger in the SMT to generate additional certificates. If you have an existing certificate or CA, you may use it instead.
Root Password: root
Server Password: server
Root File Name: root.pem
Trusted File Name: trusted.pem
Server File Name: server.pem
Company: Alcatel-Lucent (Internal)
Website: http://www.alcatel-lucent.com
City:
State:
Country: India
< Back
Next >
Cancel

9 Enter the **Root Password** and the **Server Password** to allow secure connection from SMT to the servers. The default file names and location information are displayed. If required, edit the information.

10 The 8950 AAA is installed at the selected location.

Result: On completion of the installation, the **Installation Complete** dialog box appears.

11 Click **Finish** to close the installation program, or click **Run Server Management Tool** to start the SMT to configure and manage your servers. You can also view the *Release Notes* from the **Setup Complete** dialog.

12 Install sample policy rules for the enterprise network. For more details, see Install sample policies and rules for enterprise network.

Install sample policies and rules for enterprise network

Overview

The 8950 AAA server installation package for the enterprise network comprises predefined, sample policy rules. Use these policy rules to configure the PolicyAssistant to match the requirements of the enterprise network. You can use these rules or create new rules based on these predefined rules. For more information on configuring the PolicyAssistant based on the sample rules, see Chapter 7, Configure PolicyAssistant.

Purpose

Use this procedure to install the predefined sample policy rules for the enterprise network.

Procedure

1. On Windows, navigate to *<Install-Directory>/run/samples/ebg* folder.
2. Copy all the predefined sample policies to the *<Install-Directory>/run* folder.
3. Start SMT. If SMT is already running, restart SMT.

   For more information on how to start SMT, see procedure, Start SMT on Windows platform.

4. From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant** to view the sample rules in the Policy Assistant panel
5. Modify the sample rules according to the requirement.

Start SMT on Windows platform

Choose one of the following methods to start SMT on Windows platform:

- Click **Start** button to display the **Start** menu. Select **Programs**. Navigate to the folder on which the **8950 AAA** is installed. Click **Server Management Tool**.
- Double-click the **Server management Tool** icon on the desktop.
- In the command prompt window, change directory to *<Install-Directory>/bin*, enter the following command and press **Enter**.

  ```
  aaa-smt
  ```

Part III: 8950 AAA PolicyAssistant

Overview

Purpose

This part describes the PolicyAssistant for the enterprise network. It provides procedures to configure, create, and edit a template, and procedures to configure the PolicyAssistant for various enterprise network scenarios.

Contents

This part covers the following chapters.

PolicyAssistant overview	37
Configure PolicyAssistant	41
Configure templates	101

6 PolicyAssistant overview

Overview

Purpose

This chapter provides an overview of policy, policy wizard, and PolicyAssistant used in 8950 AAA server. The PolicyAssistant is a tool to create policies to define the user access rules in the enterprise network.

Contents

This chapter covers the following topics.

PolicyAssistant	37
Policy	38
Policy Wizard	39

PolicyAssistant

PolicyAssistant helps the service providers to set up a secure access to the network resources. PolicyAssistant creates, manages, and applies policies to control how and when the users access the network.

PolicyAssistant allows you to configure 8950 AAA software through its built-in Policy Wizard. The Policy Wizard collects data on processing your request and saves it to the PolicyAssistant files.

The PolicyAssistant panel in the Server Management Tool (SMT) contains a table of available policies defined for your network.You can configure the PolicyAssistant to support multiple policies. The number of policies required depends on the following factors:

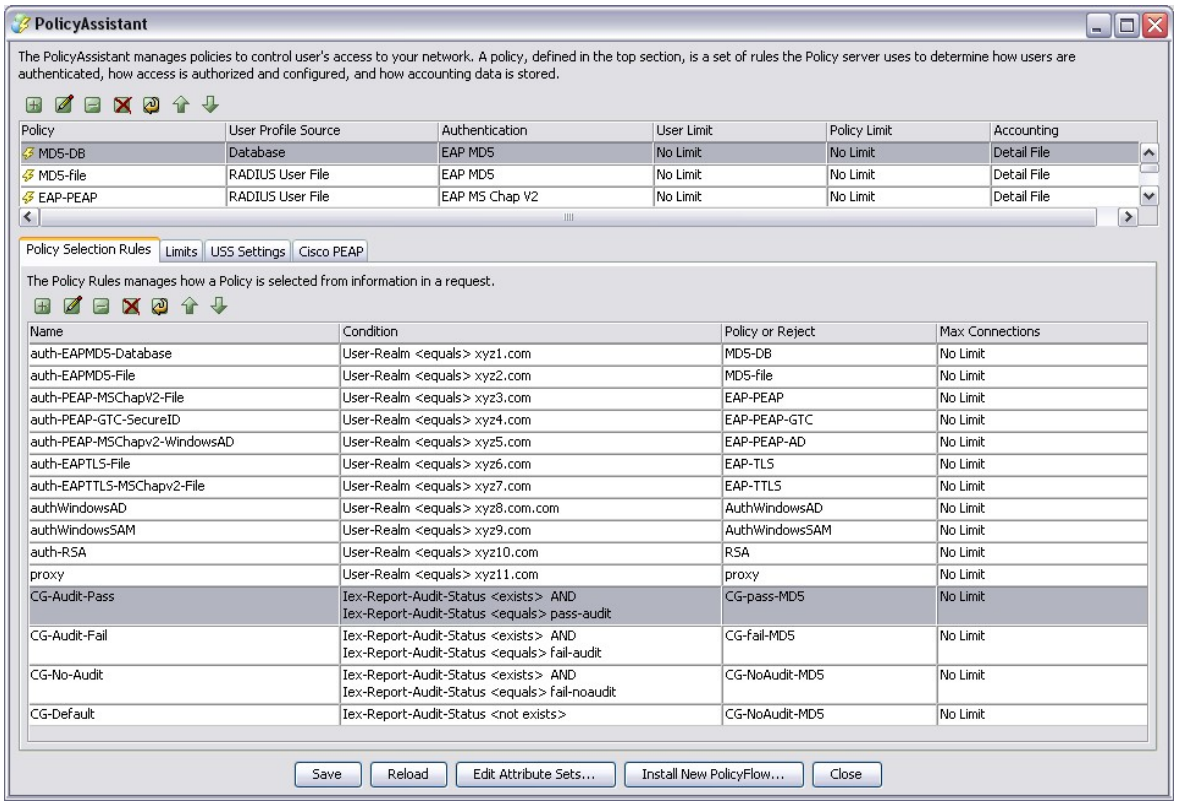
- Type of services provided by the network
- Equipment requirements

- Customer requirements
- Geographic location of the customer

Start PolicyAssistant

In the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**. The **PolicyAssistant** window opens.

Figure 6-1 PolicyAssistant


PolicyAssistant
The PolicyAssistant manages policies to control user's access to your network. A policy, defined in the top section, is a set of rules the Policy server uses to determine how users are authenticated, how access is authorized and configured, and how accounting data is stored.
Policy | User Profile Source | Authentication | User Limit | Policy Limit | Accounting
MD5-DB | Database | EAP MD5 | No Limit | No Limit | Detail File
MD5-file | RADIUS User File | EAP MD5 | No Limit | No Limit | Detail File
EAP-PEAP | RADIUS User File | EAP MS Chap V2 | No Limit | No Limit | Detail File
Policy Selection Rules
Limits
USS Settings
Cisco PEAP
The Policy Rules manages how a Policy is selected from information in a request.
Name | Condition | Policy or Reject | Max Connections
auth-EAPMD5-Database | User-Realm <equals> xyz1.com | MD5-DB | No Limit
auth-EAPMD5-File | User-Realm <equals> xyz2.com | MD5-file | No Limit
auth-PEAP-MSChapV2-File | User-Realm <equals> xyz3.com | EAP-PEAP | No Limit
auth-PEAP-GTC-SecureID | User-Realm <equals> xyz4.com | EAP-PEAP-GTC | No Limit
auth-PEAP-MSChapv2-WindowsAD | User-Realm <equals> xyz5.com | EAP-PEAP-AD | No Limit
auth-EAPTLS-File | User-Realm <equals> xyz6.com | EAP-TLS | No Limit
auth-EAPTTLS-MSChapv2-File | User-Realm <equals> xyz7.com | EAP-TTLS | No Limit
authWindowsAD | User-Realm <equals> xyz8.com.com | AuthWindowsAD | No Limit
authWindowsSAM | User-Realm <equals> xyz9.com | AuthWindowsSAM | No Limit
auth-RSA | User-Realm <equals> xyz10.com | RSA | No Limit
proxy | User-Realm <equals> xyz11.com | proxy | No Limit
CG-Audit-Pass | Iex-Report-Audit-Status <exists> AND Iex-Report-Audit-Status <equals> pass-audit | CG-pass-MD5 | No Limit
CG-Audit-Fail | Iex-Report-Audit-Status <exists> AND Iex-Report-Audit-Status <equals> fail-audit | CG-fail-MD5 | No Limit
CG-No-Audit | Iex-Report-Audit-Status <exists> AND Iex-Report-Audit-Status <equals> fail-noaudit | CG-NoAudit-MD5 | No Limit
CG-Default | Iex-Report-Audit-Status <not exists> | CG-NoAudit-MD5 | No Limit
Save
Reload
Edit Attribute Sets...
Install New PolicyFlow...
Close

The PolicyAssistant window comprises two sections. The top section allows you to create and configure new policies, and manage policies to control user access to the network. The bottom section contains four tabs that allows you to manage a selected policy.

Policy

A policy is a set of rules. The Policy server uses the policy for the following functions:

- To authenticate users
- To authorize and configure access to users
- To store the accounting data

Each policy defines the following:

- User source (the location where the user profiles are stored)

- Type of authentication that the server performs
- Policy limits
- Account information processing

Policy Wizard

Use the Policy Wizard to create policies and populate the table containing the policy information. When you run the PolicyAssistant for the first time, the table panel does not appear; instead, a Policy Wizard displays. The Policy Wizard allows you to create the first policy.

The Policy Wizard helps you to define the following information for each policy you create:

- Policy name
- Location where user profiles are stored
  The user profile list includes User Files, LDAP, Database, and so on.
- Authentication type for the user authentication
  The authentication type includes plain text passwords, EAP authentication, external authentication, secure token cards, and so on.
- A set of rules to process accounting records
- Session or policy limits applicable to the policy

7 Configure PolicyAssistant

Overview

Purpose

This chapter describes procedures to configure selected sample policies and rules using Policy Assistant wizard.

> **Note:** The Policy selection rules are defined based on the incoming RADIUS attributes to select the appropriate policy to be executed.

The pre-defined rules to configure the PolicyAssistant are located in the *..\AAA\run\samples\ebg* folder. Copy the sample, predefined policies from the samples folder before configuring the policy selection rules. For more information to copy the sample rules, see procedure, Install sample policies and rules for enterprise network.

Contents

This chapter covers the following topics.

Authentication methods	42
Configure policy selection rule	42
Configure PolicyAssistant rules for OmniSwitch	46
Configure PolicyAssistant rules for CyberGateKeeper	87
Configure policy selection rules for CyberGateKeeper	94

Authentication methods

This topic describes the different authentication methods used in the enterprise network.

EAP-MD5

This method is used to authenticate the 802.1x user credentials using MD5 hash mechanism.

EAP-TLS

This method is used to authenticate user devices using certificates. In this mechanism, both the server and client certificates are verified mutually.

EAP-TTLS, EAP-PEAP

Both these methods use X.509 certificates to create a secure tunnel inside which user credentials are authenticated. Two of the internal authentication modes are as follows:

- **EAP-MSChapV2,** which authenticates the user credentials against Windows SAM.
- **EAP-GTC,** where the user credentials are authenticated against RSA Ace server.

Authenticate against RSA/ACE server

Two of the authentication methods are as follows:

- **PAP**: Using this method, the 8950 AAA contacts the RSA/ACE server to authenticate the user credentials.
- **EAP-PEAP-GTC**: The 8950 AAA creates an outer tunnel and inside this tunnel, GTC is used to authenticate the user credentials against RSA/ACE server. This method overcomes the defects in the PAP method.

Configure policy selection rule

Purpose

Use this procedure to configure a policy selection rule.

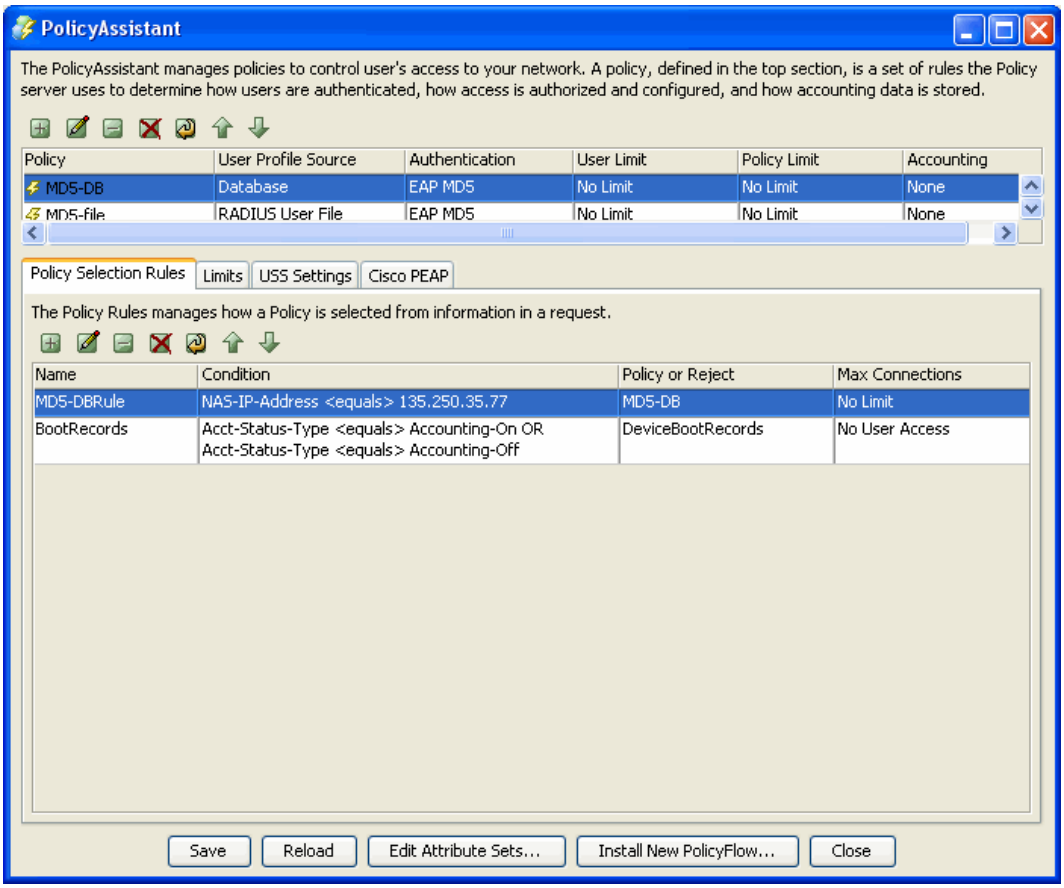
Note: The procedure details a sample rule definition. Define an appropriate rule to choose a required policy. For more detailed configuration procedures, see the PolicyAssistant User Guide in the *Documentation* section at http://www.8950aaa.com/.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant.**

Result: The **PolicyAssistant** window opens.

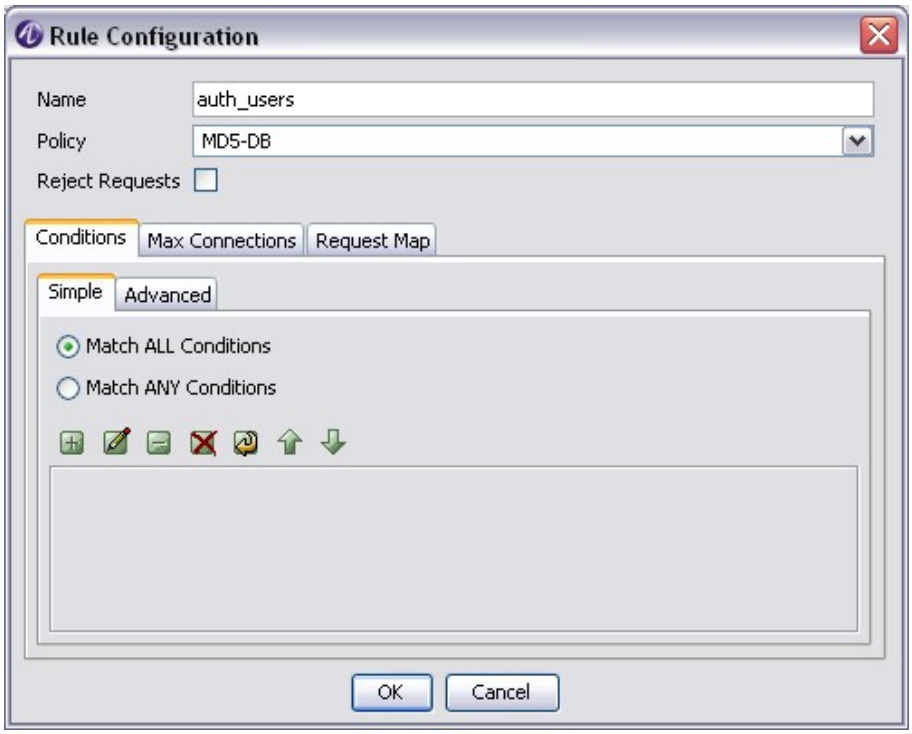
Figure 7-1 PolicyAssistant



2 From the **Policy Selection Rules** tab of the **PolicyAssistant** window, click .

Result: The **Rule Configuration** window opens.

Figure 7-2 Rule Configuration



3 Perform the following steps:

a. Enter a name for the rule.

b. From the **Policy** drop-down list, select the required policy.

c. Click **Conditions** tab.

Result: The **Conditions** panel opens. See Figure 7-2.

4 Click **Simple** tab and perform the following steps:

a. Select **Match ALL Conditions** or **Match Any Conditions** as per your requirements.

b. Click .

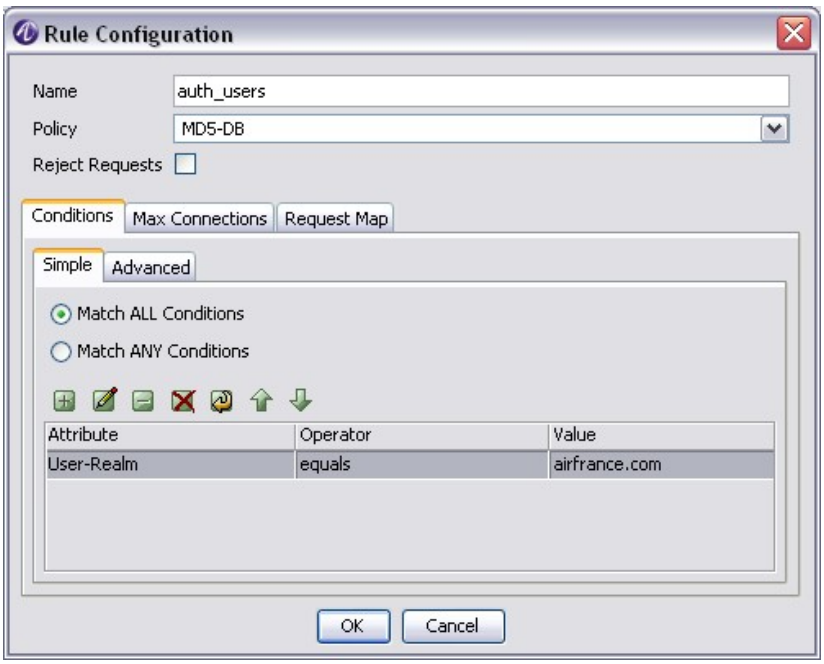
Result: The **Conditions** window opens.

Figure 7-3 Conditions

5 Select the attribute, set the condition, and enter the corresponding value. Click **OK**.

Result: The specified condition displays in the **Simple** panel.

Figure 7-4 Simple panel



6 Click **OK** to complete.

Note: Rules are defined based on the requirement to choose the appropriate policy.

Configure PolicyAssistant rules for OmniSwitch

This section contains procedures to configure the PolicyAssistant for different OmniSwitch policies. The PolicyAssistant allows the following tasks on the sample rules:

1. **Create a rule:** From Figure 6-1, click to create policy rules to configure the PolicyAssistant.
2. **Copy an existing sample rule:** From Figure 6-1, select the required rule and click to copy the rule. You can modify and save the rule under a different name.
3. **Edit an existing sample rule:** From Figure 6-1, select the required rule and click to edit the rule.

The following procedures are sample configuration procedures to help you to configure the PolicyAssistant for different RADIUS clients in the enterprise network. These procedures illustrate how you can choose a user profile source and an authentication method. You can follow these procedures to create rules based on the existing sample rules. Ensure to save them under a different name.

Configure EAP-MD5 authentication with Database as user source

Purpose

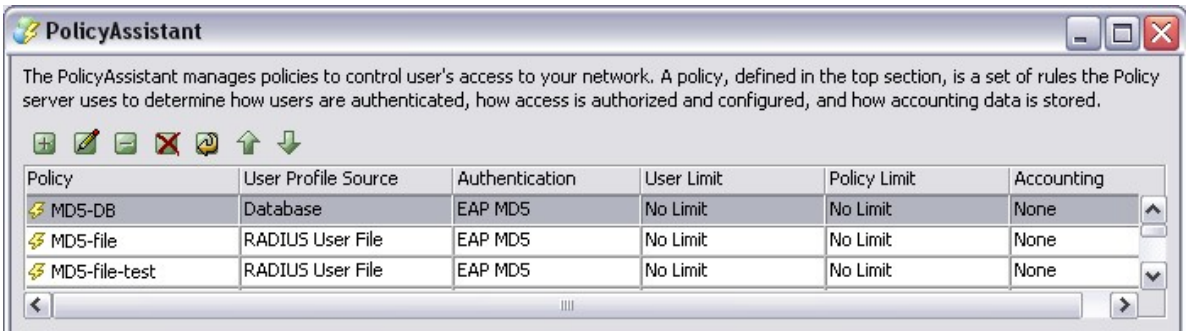
Use this procedure to configure EAP-MD5 authentication with database as user source using PolicyAssistant.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens.

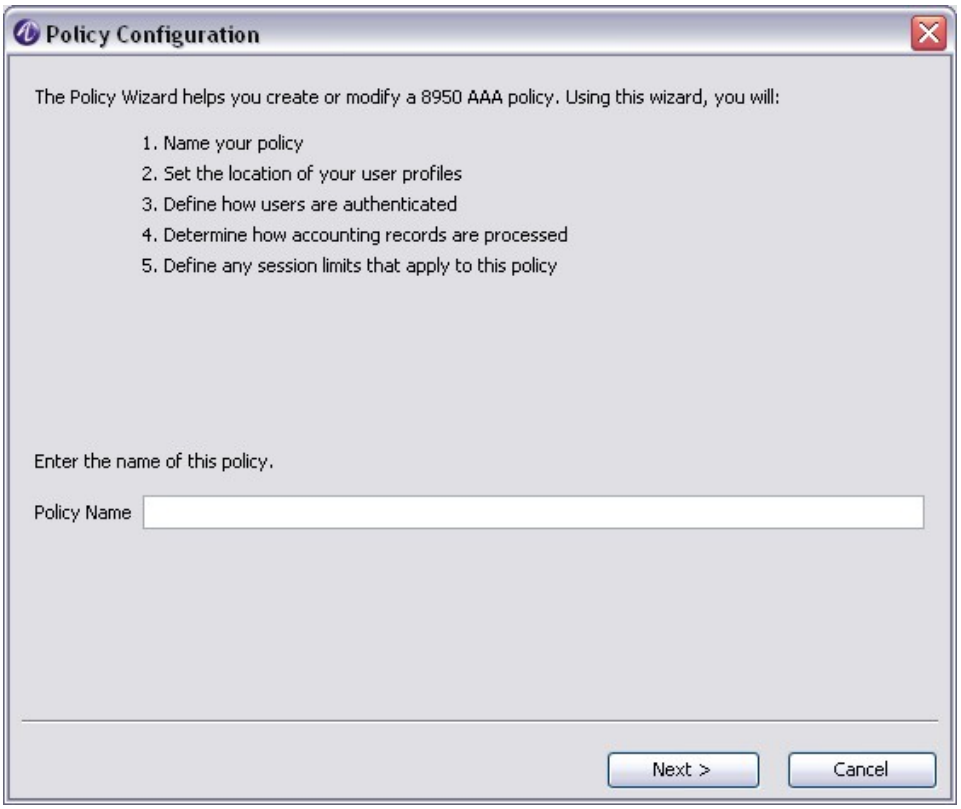
Figure 7-5 PolicyAssistant



2 Click to add a new policy.

Result: The **Policy Configuration** window opens.

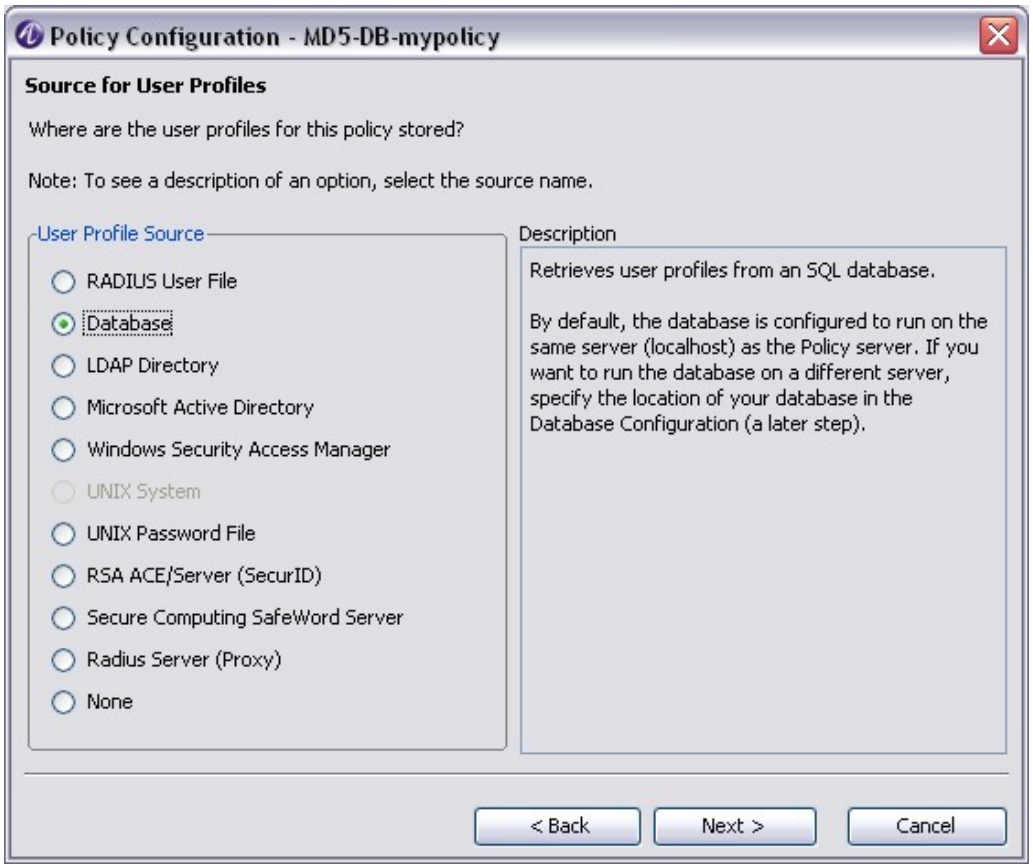
Figure 7-6 Policy Configuration


Policy Configuration
The Policy Wizard helps you create or modify a 8950 AAA policy. Using this wizard, you will:
1. Name your policy
2. Set the location of your user profiles
3. Define how users are authenticated
4. Determine how accounting records are processed
5. Define any session limits that apply to this policy
Enter the name of this policy.
Policy Name
Next >
Cancel

3 Enter a new name for your policy. For example, enter the policy name as *MD5-DB-mypolicy*. Click **Next.**

Result: The **Source for User Profiles** window opens.

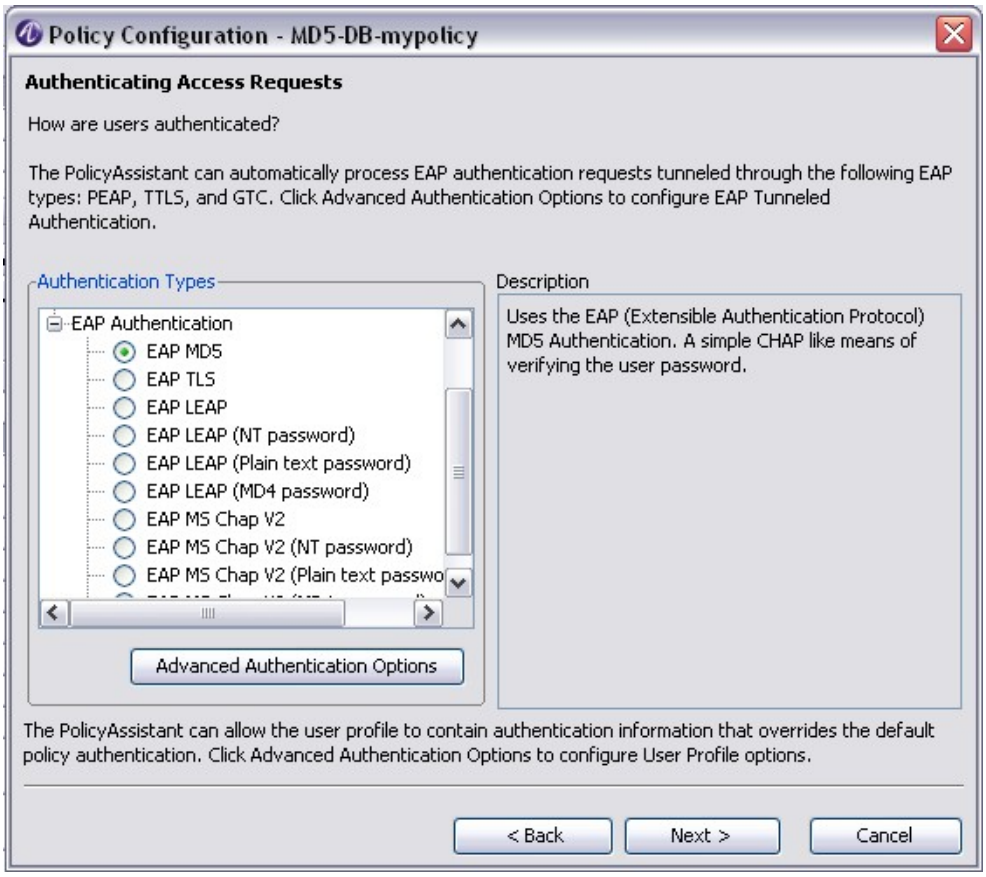
Figure 7-7 Source for User Profiles


Policy Configuration - MD5-DB-mypolicy
Source for User Profiles
Where are the user profiles for this policy stored?
Note: To see a description of an option, select the source name.
User Profile Source
RADIUS User File
Database
LDAP Directory
Microsoft Active Directory
Windows Security Access Manager
UNIX System
UNIX Password File
RSA ACE/Server (SecurID)
Secure Computing SafeWord Server
Radius Server (Proxy)
None
Description
Retrieves user profiles from an SQL database.
By default, the database is configured to run on the same server (localhost) as the Policy server. If you want to run the database on a different server, specify the location of your database in the Database Configuration (a later step).
< Back
Next >
Cancel

4 Select **Database** and click **Next.**

Result: The **Authenticating Access Requests** window opens.

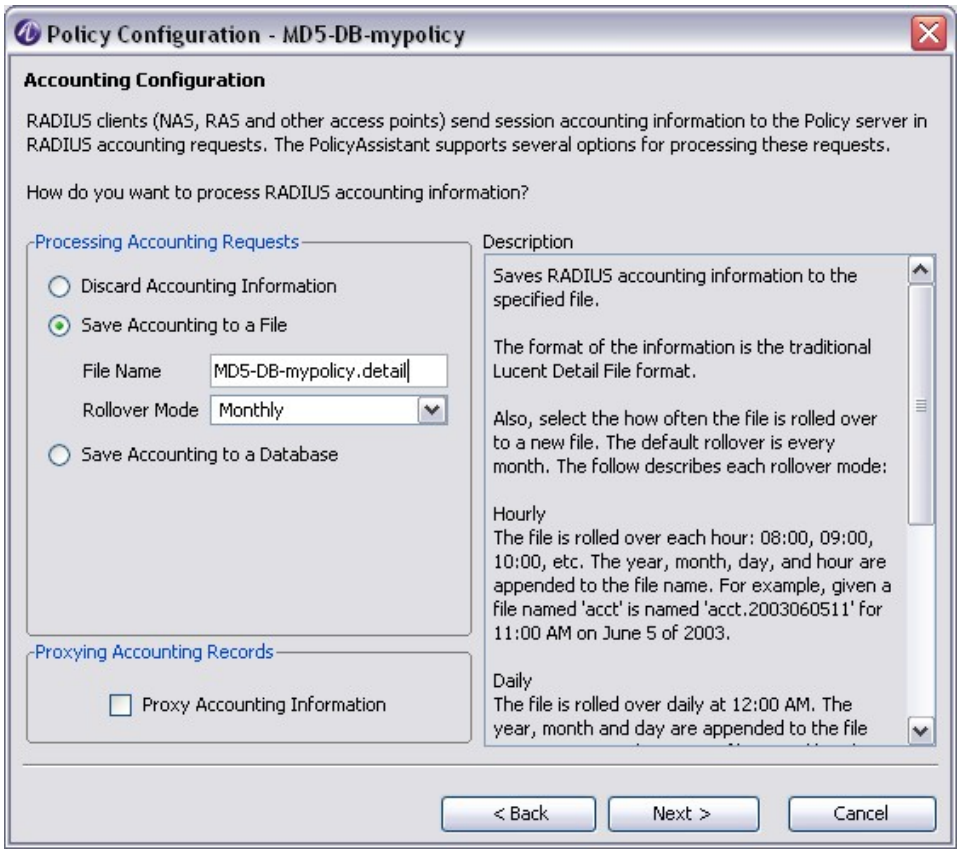
Figure 7-8 Authenticating Access Requests


Policy Configuration - MD5-DB-mypolicy
Authenticating Access Requests
How are users authenticated?
The PolicyAssistant can automatically process EAP authentication requests tunneled through the following EAP types: PEAP, TTLS, and GTC. Click Advanced Authentication Options to configure EAP Tunneled Authentication.
Authentication Types
EAP Authentication
EAP MD5
EAP TLS
EAP LEAP
EAP LEAP (NT password)
EAP LEAP (Plain text password)
EAP LEAP (MD4 password)
EAP MS Chap V2
EAP MS Chap V2 (NT password)
EAP MS Chap V2 (Plain text passwo
Advanced Authentication Options
Description
Uses the EAP (Extensible Authentication Protocol) MD5 Authentication. A simple CHAP like means of verifying the user password.
The PolicyAssistant can allow the user profile to contain authentication information that overrides the default policy authentication. Click Advanced Authentication Options to configure User Profile options.
< Back
Next >
Cancel

5 Expand **EAP Authentication** in the list of **Authentication Types**, select **EAP MD5,** and click **Next**.

Result: The **Accounting Configuration** window opens.

Figure 7-9 Accounting Configuration


Policy Configuration - MD5-DB-mypolicy
Accounting Configuration
RADIUS clients (NAS, RAS and other access points) send session accounting information to the Policy server in RADIUS accounting requests. The PolicyAssistant supports several options for processing these requests.
How do you want to process RADIUS accounting information?
Processing Accounting Requests
Discard Accounting Information
Save Accounting to a File
File Name
MD5-DB-mypolicy.detail
Rollover Mode
Monthly
Save Accounting to a Database
Proxying Accounting Records
Proxy Accounting Information
Description
Saves RADIUS accounting information to the specified file.
The format of the information is the traditional Lucent Detail File format.
Also, select the how often the file is rolled over to a new file. The default rollover is every month. The follow describes each rollover mode:
Hourly
The file is rolled over each hour: 08:00, 09:00, 10:00, etc. The year, month, day, and hour are appended to the file name. For example, given a file named 'acct' is named 'acct.2003060511' for 11:00 AM on June 5 of 2003.
Daily
The file is rolled over daily at 12:00 AM. The year, month and day are appended to the file
< Back
Next >
Cancel

6 Select **Save Accounting to a File** and perform the following steps:

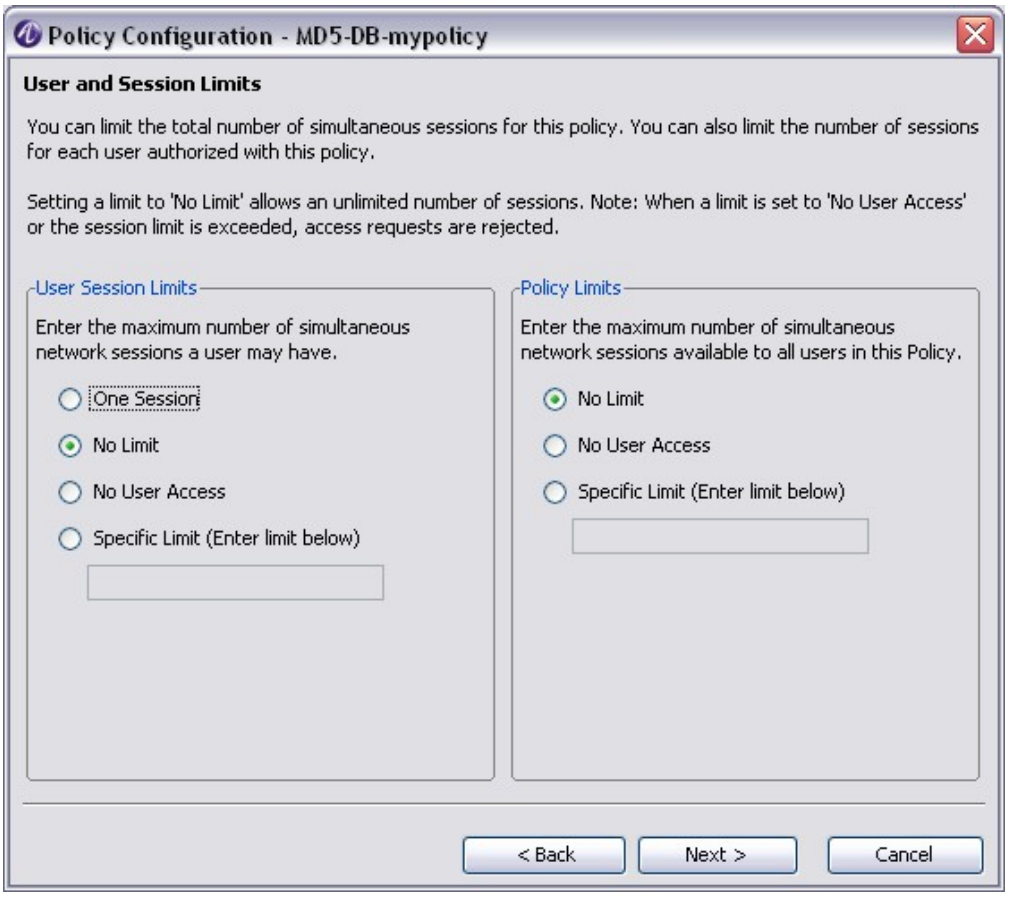
a. The file name appears by default. If needed, modify the file name.

b. Select the rollover mode.

c. Click **Next**.

Result: The **User and Session Limits** window opens.

Figure 7-10 User and Session Limits


Policy Configuration - MD5-DB-mypolicy
User and Session Limits
You can limit the total number of simultaneous sessions for this policy. You can also limit the number of sessions for each user authorized with this policy.
Setting a limit to 'No Limit' allows an unlimited number of sessions. Note: When a limit is set to 'No User Access' or the session limit is exceeded, access requests are rejected.
User Session Limits
Enter the maximum number of simultaneous network sessions a user may have.
One Session
No Limit
No User Access
Specific Limit (Enter limit below)
Policy Limits
Enter the maximum number of simultaneous network sessions available to all users in this Policy.
No Limit
No User Access
Specific Limit (Enter limit below)
< Back
Next >
Cancel

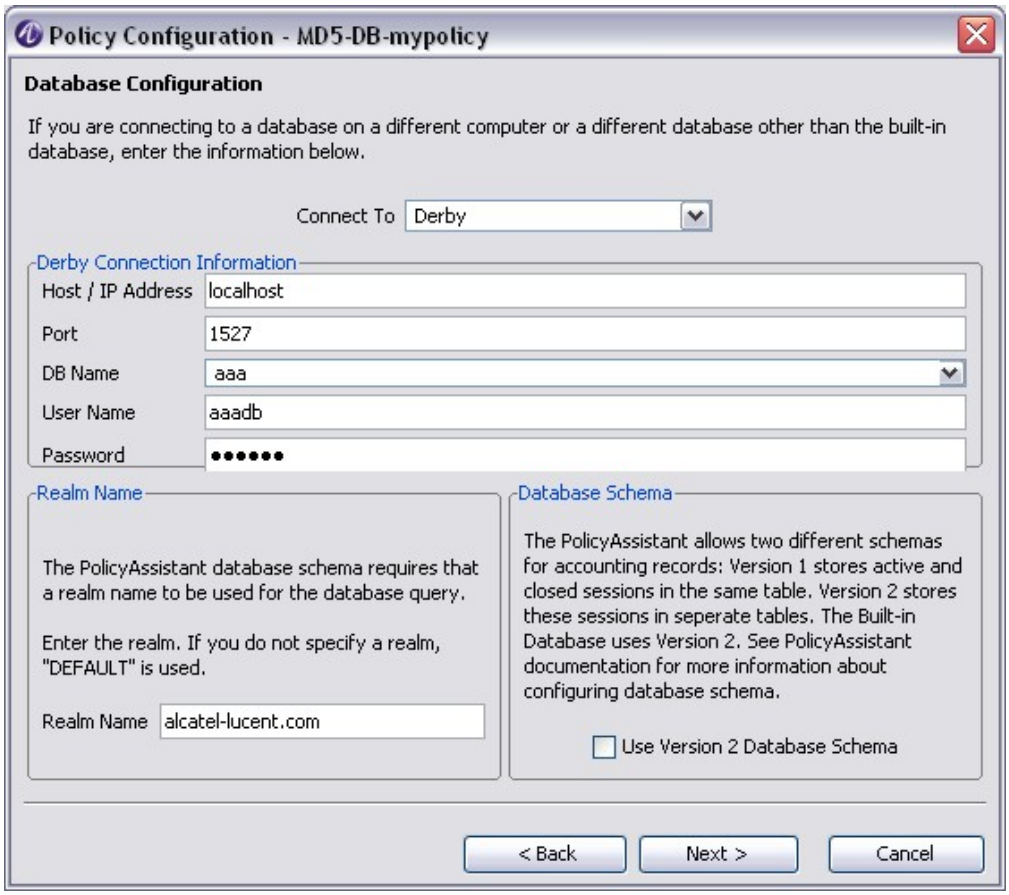
7 Enter the following details and click **Next**.

a. In the **User Session Limits** panel, select **No Limit**.

b. In the **Policy Limits** panel, select **No Limit**.

Result: The **Database Configuration** window opens.

Figure 7-11 Database Configuration


Policy Configuration - MD5-DB-mypolicy
Database Configuration
If you are connecting to a database on a different computer or a different database other than the built-in database, enter the information below.
Connect To
Derby
Derby Connection Information
Host / IP Address
localhost
Port
1527
DB Name
aaa
User Name
aaadb
Password
Realm Name
The PolicyAssistant database schema requires that a realm name to be used for the database query.
Enter the realm. If you do not specify a realm, "DEFAULT" is used.
Realm Name
alcatel-lucent.com
Database Schema
The PolicyAssistant allows two different schemas for accounting records: Version 1 stores active and closed sessions in the same table. Version 2 stores these sessions in seperate tables. The Built-in Database uses Version 2. See PolicyAssistant documentation for more information about configuring database schema.
Use Version 2 Database Schema
< Back
Next >
Cancel

8 Depending upon the type of database selected in the **Connect To** drop-down list, the connection information changes.

For example, if you choose to connect to Derby database, enter the following database host details and click **Next**.

a. Enter the hostname or IP Address of the host.

b. Enter the database port.

c. Enter the database name.

d. Enter the username to access the database.

e. Enter the password.

f. Enter the realm name. User records in the database should correspond with the realm name entered here.

Result: The **Attribute Set for Policy** window opens.

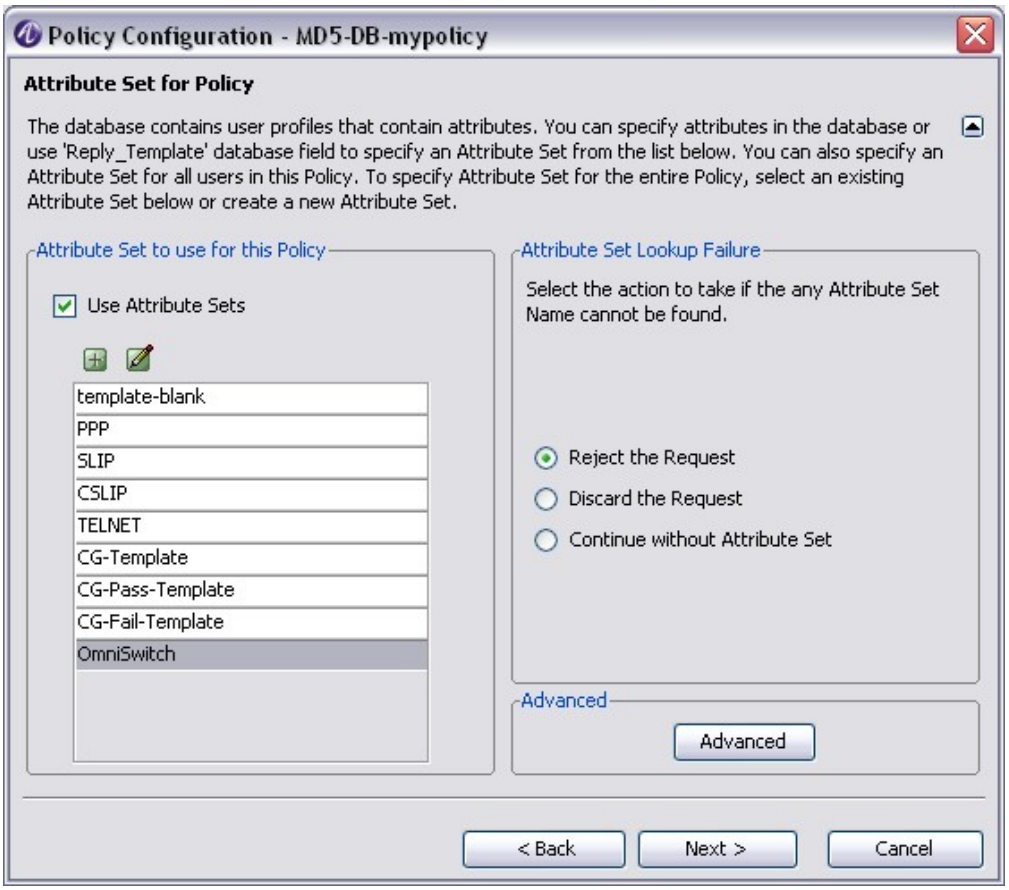
9 Perform the following steps in the window.

a. Check **Use Attribute Set**.

b. From the list of templates, select **OmniSwitch**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failure** section, select **Reject the Request**.

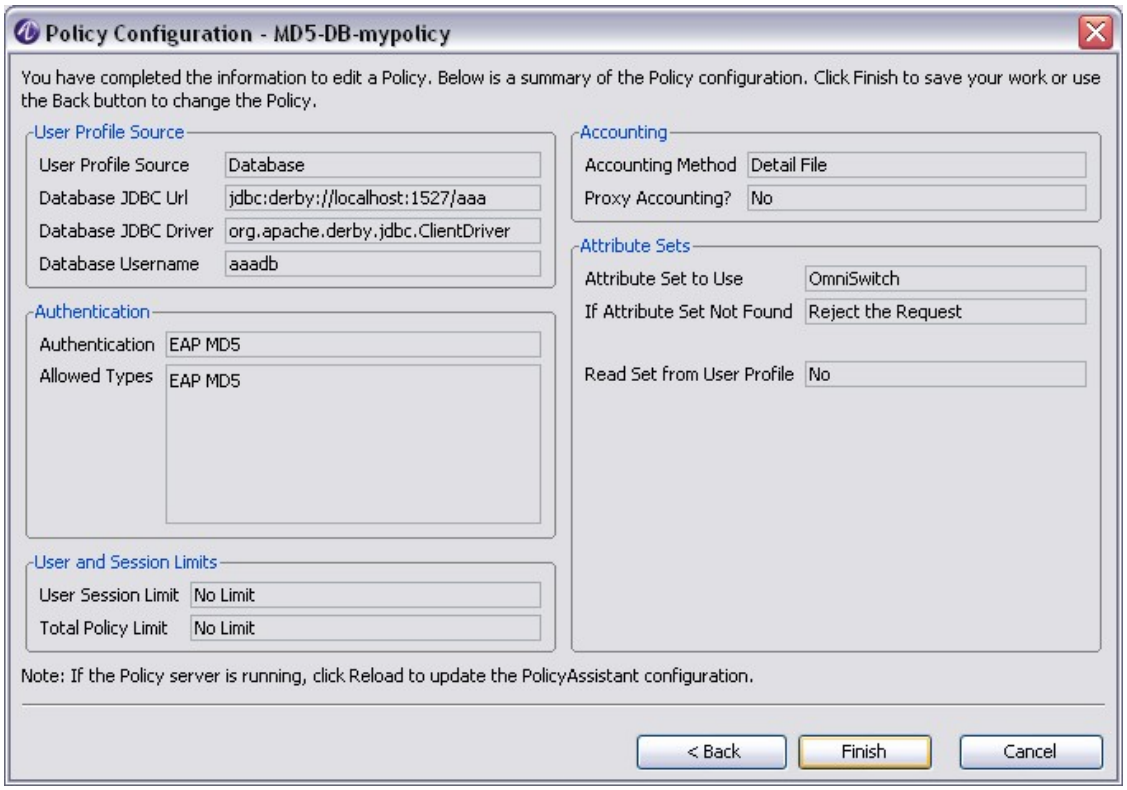
Figure 7-12 Attribute Set for Policy


Policy Configuration - MD5-DB-mypolicy
Attribute Set for Policy
The database contains user profiles that contain attributes. You can specify attributes in the database or use 'Reply_Template' database field to specify an Attribute Set from the list below. You can also specify an Attribute Set for all users in this Policy. To specify Attribute Set for the entire Policy, select an existing Attribute Set below or create a new Attribute Set.
Attribute Set to use for this Policy
Use Attribute Sets
template-blank
PPP
SLIP
CSLIP
TELNET
CG-Template
CG-Pass-Template
CG-Fail-Template
OmniSwitch
Attribute Set Lookup Failure
Select the action to take if the any Attribute Set Name cannot be found.
Reject the Request
Discard the Request
Continue without Attribute Set
Advanced
Advanced
< Back
Next >
Cancel

d. Click N**ext**.

Result: A window with a summary of policy configuration opens.

Figure 7-13 Policy configuration summary


Policy Configuration - MD5-DB-mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source Database
Database JDBC Url jdbc:derby://localhost:1527/aaa
Database JDBC Driver org.apache.derby.jdbc.ClientDriver
Database Username aaadb
Authentication
Authentication EAP MD5
Allowed Types EAP MD5
User and Session Limits
User Session Limit No Limit
Total Policy Limit No Limit
Accounting
Accounting Method Detail File
Proxy Accounting? No
Attribute Sets
Attribute Set to Use OmniSwitch
If Attribute Set Not Found Reject the Request
Read Set from User Profile No
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

10 Click **Finish** to complete the PolicyAssistant configuration.

11 Click **Save** to save the policy created.

Configure EAP-MD5 authentication with RADIUS User File as user source

Purpose

Use this procedure to configure EAP-MD5 authentication with RADIUS user file as user source using PolicyAssistant.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens. See Figure 7-5.

2 Click to add a new policy.

Result: The **Policy Configuration** window opens. See Figure 7-6.

3 Enter a new name for your policy. For example, enter the policy name as *MD5-radiusfile-mypolicy*. Click **Next**.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

4 Select **Radius User File** and click **Next**.

Result: The **Authentication Access Requests** window opens. See Figure 7-8.

5 Expand **EAP Authentication** in the list of **Authentication Types**, select **EAP MD5** and click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9.

6 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.
b. Select the rollover mode.
c. Click **Next**.

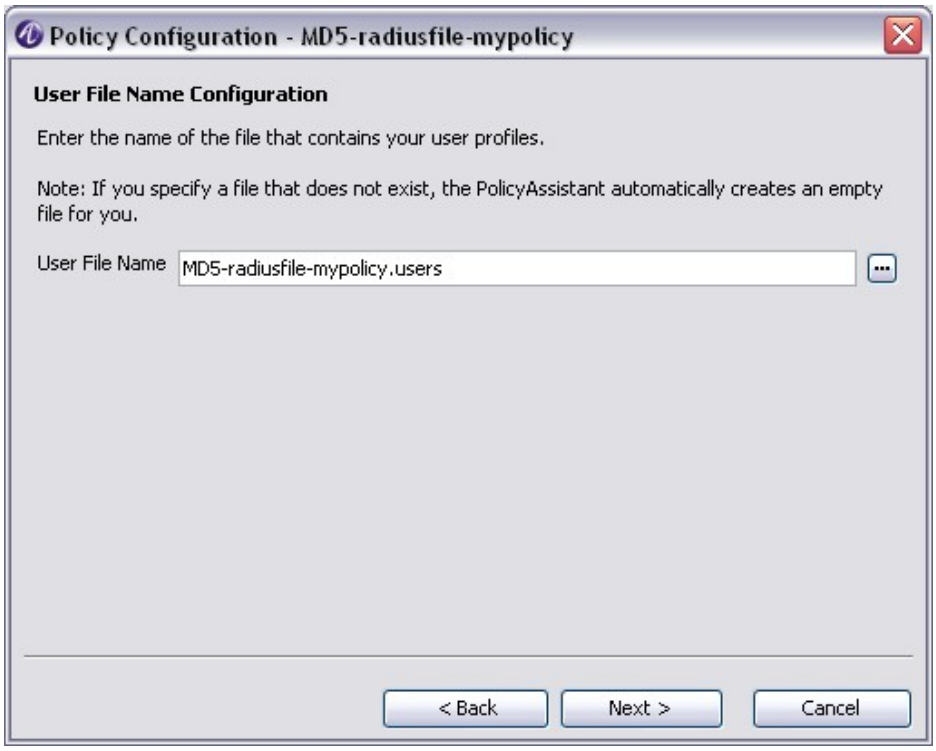
Result: The **User and Session Limits** window opens. See Figure 7-10.

7 Perform the following steps:

a. In the **User Session Limits** section, select **No Limit**.
b. In the **Policy Limits** section, select **No Limit**.
c. Click **Next**.

Result: The **User File Name Configuration** window opens.

Figure 7-14 User File Name Configuration


Policy Configuration - MD5-radiusfile-mypolicy
User File Name Configuration
Enter the name of the file that contains your user profiles.
Note: If you specify a file that does not exist, the PolicyAssistant automatically creates an empty file for you.
User File Name
MD5-radiusfile-mypolicy.users
< Back
Next >
Cancel

8 The user file name appears by default. If needed, modify the user file name and click **Next**.

Result: The **Attribute Set for Policy** window opens. See Figure 7-12.

9 Perform the following steps:

a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.

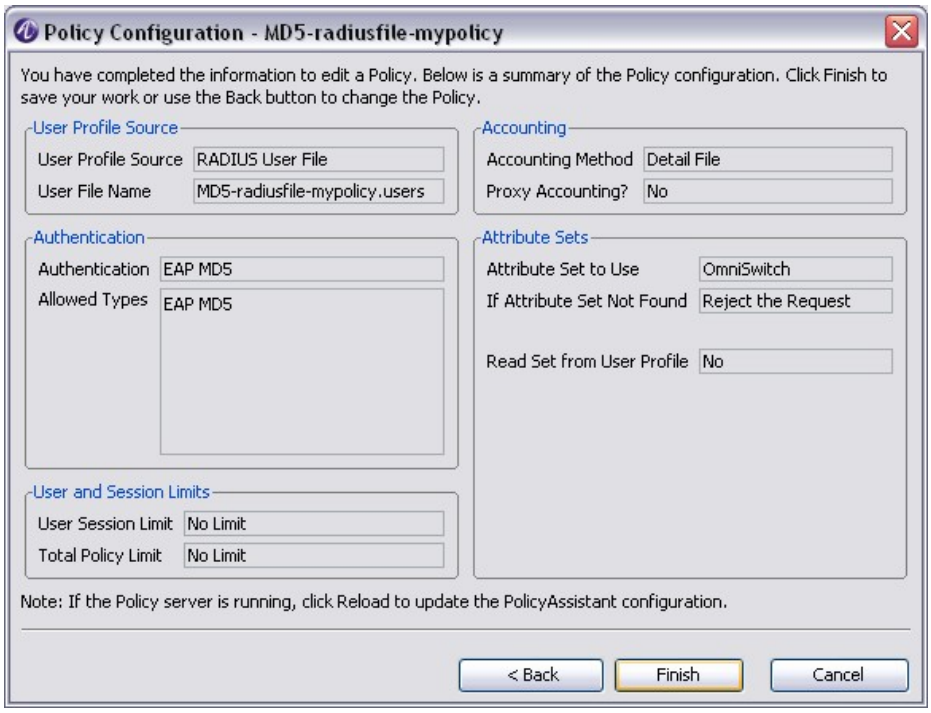
b. From the list of templates, select **OmniSwitch**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failure** section, select **Reject the Request**.

d. Click **Next**.

Result: A window with a summary of policy configuration opens.

Figure 7-15 Policy configuration summary


Policy Configuration - MD5-radiusfile-mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source RADIUS User File
User File Name MD5-radiusfile-mypolicy.users
Accounting
Accounting Method Detail File
Proxy Accounting? No
Authentication
Authentication EAP MD5
Allowed Types EAP MD5
Attribute Sets
Attribute Set to Use OmniSwitch
If Attribute Set Not Found Reject the Request
Read Set from User Profile No
User and Session Limits
User Session Limit No Limit
Total Policy Limit No Limit
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

10 Click **Finish** to complete the PolicyAssistant configuration.

11 Click **Save** to save the policy created.

Configure EAP-PEAP-MS-CHAPv2 authentication with RADIUS User File as user source

Purpose

Use this procedure to configure EAP-PEAP-MSChapV2 as inner authentication and no CRL checking) authentication with RADIUS user file as user source using PolicyAssistant.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens. See Figure 7-5.

2 Click to add a new policy.

Result: The **Policy Configuration** window opens. See Figure 7-6.

3 Enter a new name for your policy. For example, enter the policy name as *EAP-PEAP-MSCHAPv2-mypolicy*. Click **Next**.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

4 Select **RADIUS User File** and click **Next**.

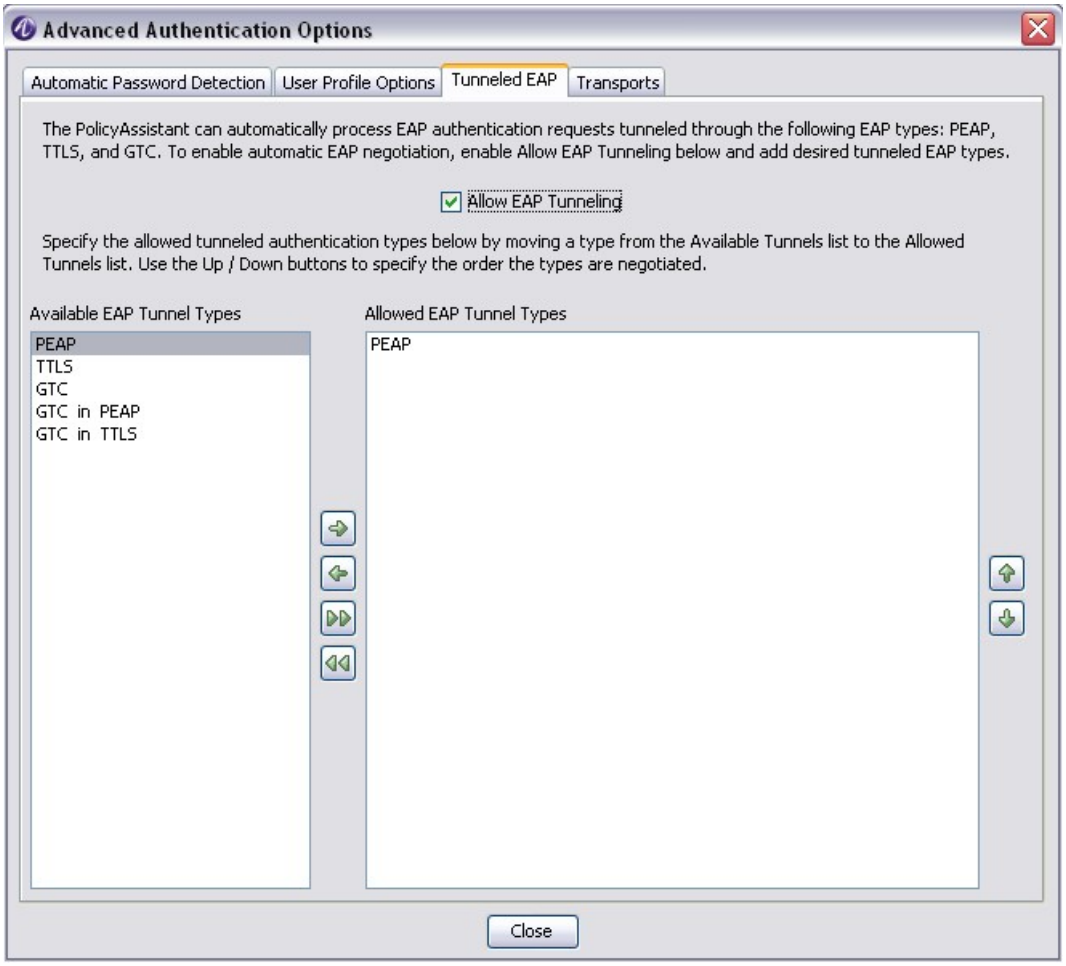
Result: The **Authentication Access Requests** window opens. See Figure 7-8.

5 Perform the following steps:

a. Expand **EAP Authentication** in the list of **Authentication Types** and select **EAP MS Chap V2**.

b. Click **Advanced Authentication Options** tab.

Figure 7-16 Advanced Authentication Options


Advanced Authentication Options
Automatic Password Detection
User Profile Options
Tunneled EAP
Transports
The PolicyAssistant can automatically process EAP authentication requests tunneled through the following EAP types: PEAP, TTLS, and GTC. To enable automatic EAP negotiation, enable Allow EAP Tunneling below and add desired tunneled EAP types.
Allow EAP Tunneling
Specify the allowed tunneled authentication types below by moving a type from the Available Tunnels list to the Allowed Tunnels list. Use the Up / Down buttons to specify the order the types are negotiated.
Available EAP Tunnel Types
PEAP
TTLS
GTC
GTC in PEAP
GTC in TTLS
Allowed EAP Tunnel Types
PEAP
Close

c. In the **Advanced Authentication Options** window, select **Tunneled EAP** tab.

d. Select **Allow EAP Tunneling**.

e. From the **Available EAP Tunnel Types** section, select **PEAP** and click .

f. Click **Close**.

g. Click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9**.**

6 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.

b. Select the rollover mode.

c. Click **Next**.

Result: The **User and Session Limits** window opens. See Figure 7-10.

7 Perform the following steps and click **Next**.

a. In the **User Session Limits** section, select **No Limit**.

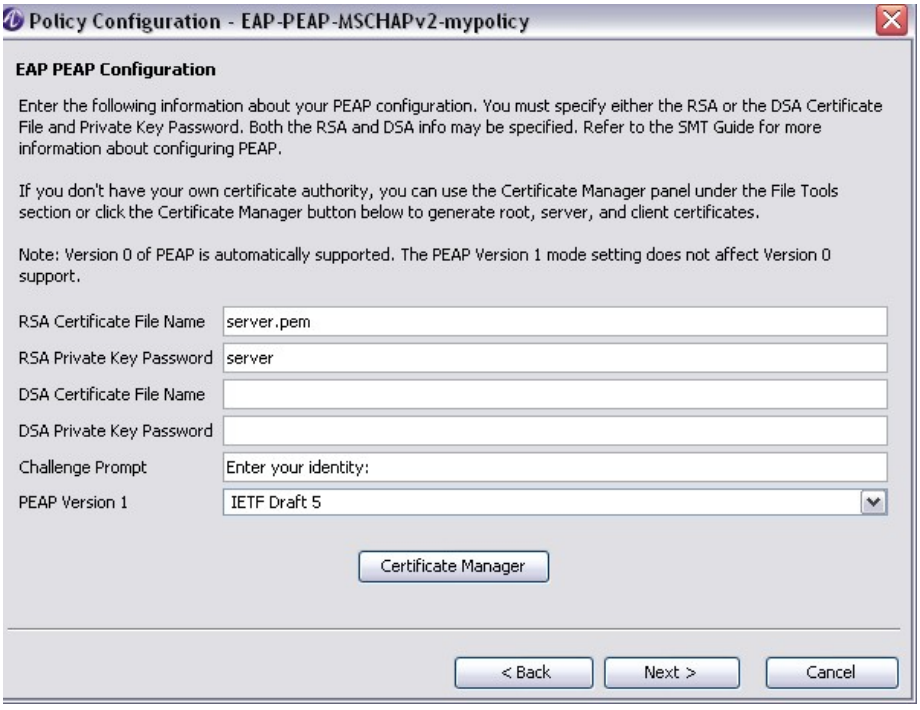
b. In the **Policy Limits** section, select **No Limit**.

Result: The **User File Name Configuration** window opens. See Figure 7-14.

8 The user file name appears by default. If needed, modify the user file name and click **Next**.

Result: The **EAP PEAP Configuration** window opens.

Figure 7-17 EAP PEAP Configuration


Policy Configuration - EAP-PEAP-MSCHAPv2-mypolicy
EAP PEAP Configuration
Enter the following information about your PEAP configuration. You must specify either the RSA or the DSA Certificate File and Private Key Password. Both the RSA and DSA info may be specified. Refer to the SMT Guide for more information about configuring PEAP.
If you don't have your own certificate authority, you can use the Certificate Manager panel under the File Tools section or click the Certificate Manager button below to generate root, server, and client certificates.
Note: Version 0 of PEAP is automatically supported. The PEAP Version 1 mode setting does not affect Version 0 support.
RSA Certificate File Name
server.pem
RSA Private Key Password
server
DSA Certificate File Name
DSA Private Key Password
Challenge Prompt
Enter your identity:
PEAP Version 1
IETF Draft 5
Certificate Manager
< Back
Next >
Cancel

9 Perform the following steps and click **Next**.

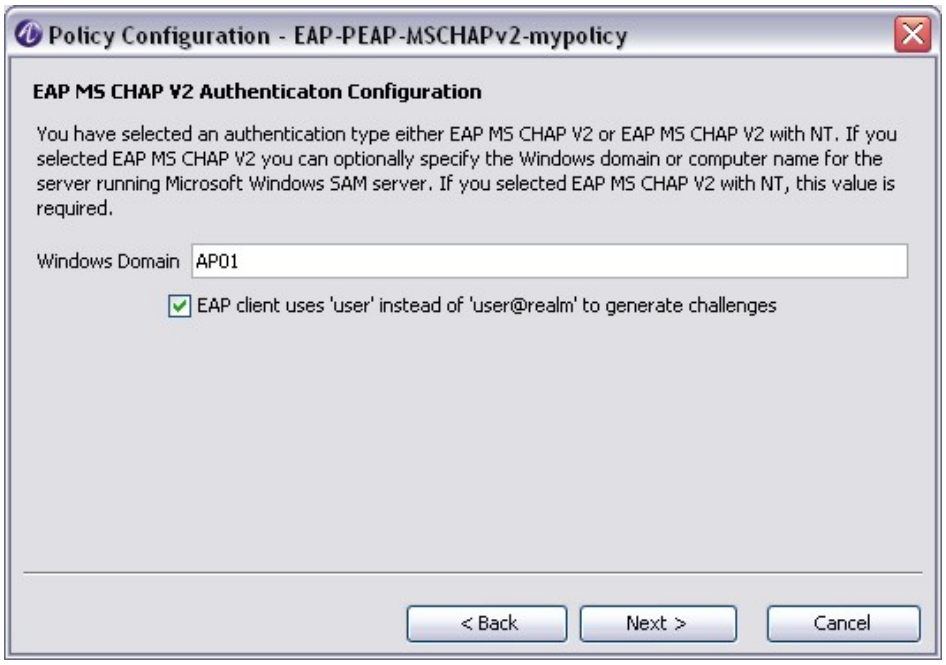
a. Enter the certificate file name and private key password for RSA or DSA.

b. Enter the challenge prompt.

c. Specify the compatibility mode for PEAP Version1.

Result: The **EAP MS CHAP V2 Authentication Configuration** window opens.

Figure 7-18 EAP MS CHAP V2 Authentication Configuration


Policy Configuration - EAP-PEAP-MSCHAPv2-mypolicy
EAP MS CHAP V2 Authenticaton Configuration
You have selected an authentication type either EAP MS CHAP V2 or EAP MS CHAP V2 with NT. If you selected EAP MS CHAP V2 you can optionally specify the Windows domain or computer name for the server running Microsoft Windows SAM server. If you selected EAP MS CHAP V2 with NT, this value is required.
Windows Domain
AP01
EAP client uses 'user' instead of 'user@realm' to generate challenges
< Back
Next >
Cancel

10 Perform the following steps:

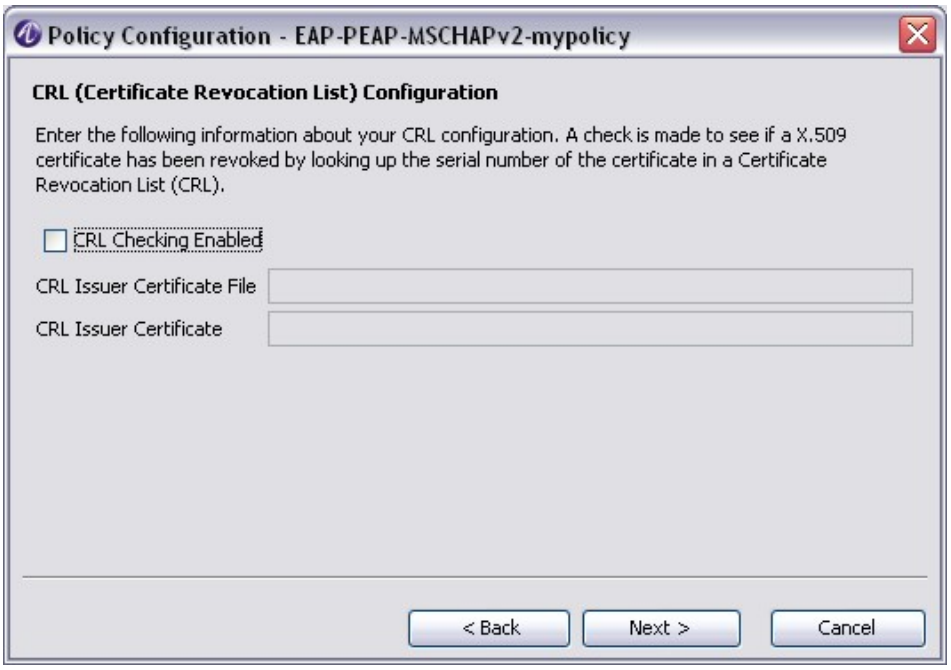
a. Enter the Windows domain or computer name on which the Microsoft Windows SAM server is running. Enter the domain or computer name only if EAP MS Chap V2 (NT Password) is chosen.

b. Select **EAP client uses user instead of user@realm to generate challenges**.

c. Click **Next**.

Result: The **CRL (Certificate Revocation List) Configuration** window opens.

Figure 7-19 CRL (Certificate Revocation List) Configuration


Policy Configuration - EAP-PEAP-MSCHAPv2-mypolicy
CRL (Certificate Revocation List) Configuration
Enter the following information about your CRL configuration. A check is made to see if a X.509 certificate has been revoked by looking up the serial number of the certificate in a Certificate Revocation List (CRL).
CRL Checking Enabled
CRL Issuer Certificate File
CRL Issuer Certificate
< Back
Next >
Cancel

11 Click **Next**.

Result: The **Attribute Set for Policy** window opens. See Figure 7-12.

12 Perform the following steps and click **Next**.

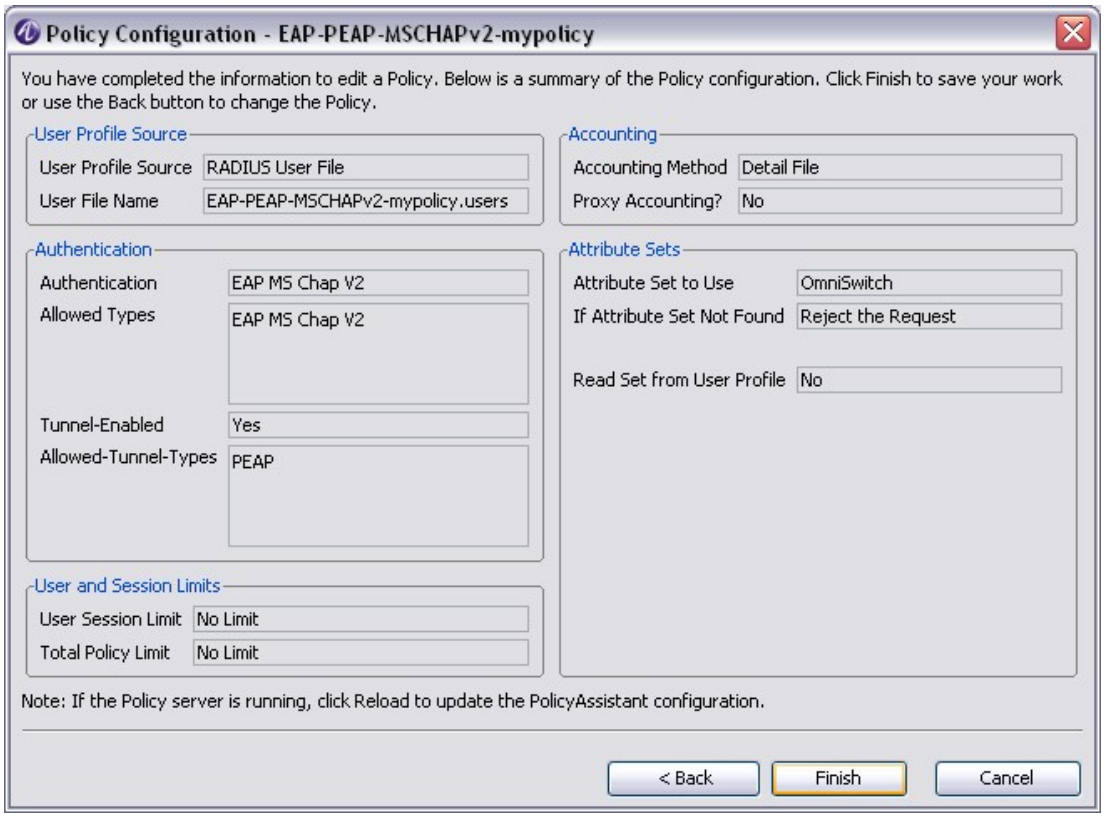
a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.

b. From the list of templates, select **OmniSwitch**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failure** section, select **Reject the Request**.

Result: A window with a summary of the policy configuration opens.

Figure 7-20 Policy configuration summary


Policy Configuration - EAP-PEAP-MSCHAPv2-mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source RADIUS User File
User File Name EAP-PEAP-MSCHAPv2-mypolicy.users
Accounting
Accounting Method Detail File
Proxy Accounting? No
Authentication
Authentication EAP MS Chap V2
Allowed Types EAP MS Chap V2
Tunnel-Enabled Yes
Allowed-Tunnel-Types PEAP
Attribute Sets
Attribute Set to Use OmniSwitch
If Attribute Set Not Found Reject the Request
Read Set from User Profile No
User and Session Limits
User Session Limit No Limit
Total Policy Limit No Limit
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

13 Click **Finish** to complete the PolicyAssistant configuration.

14 Click **Save** to save the policy created.

Configure EAP-PEAP-GTC authentication

Use this procedure to configure EAP-PEAP-GTC using PolicyAssistant. Users are authenticated against Secure ID server.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens. See Figure 7-5.

2 Click to add a new policy.

Result: The **Policy Configuration** window opens. See Figure 7-6.

3 Enter a new name for your policy. For example, enter the policy name as *EAP-PEAP-GTC-mypolicy*. Click **Next**.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

4 Select **None** and click **Next**.

Result: The **Authenticating Access Requests** window opens. See Figure 7-8.

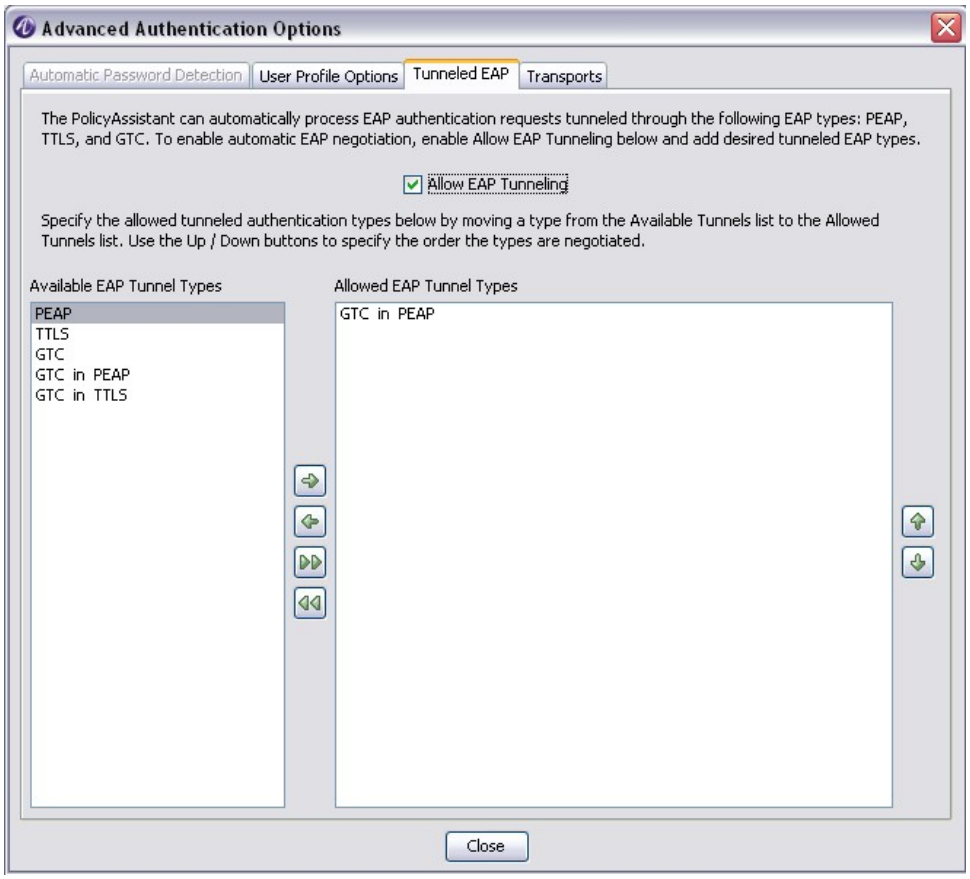
5 Expand **External Authentications** and select **RSA ACE/Server (SecureID)** and click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9.

6 Perform the following steps:

a. Click **Advanced Authentication Option**.

Figure 7-21 Advanced Authentication Options


Advanced Authentication Options
Automatic Password Detection
User Profile Options
Tunneled EAP
Transports
The PolicyAssistant can automatically process EAP authentication requests tunneled through the following EAP types: PEAP, TTLS, and GTC. To enable automatic EAP negotiation, enable Allow EAP Tunneling below and add desired tunneled EAP types.
Allow EAP Tunneling
Specify the allowed tunneled authentication types below by moving a type from the Available Tunnels list to the Allowed Tunnels list. Use the Up / Down buttons to specify the order the types are negotiated.
Available EAP Tunnel Types
PEAP
TTLS
GTC
GTC in PEAP
GTC in TTLS
Allowed EAP Tunnel Types
GTC in PEAP
Close

b. Select **EAP Tunneling**.

c. Select **GTC in PEAP** in **Allowed EAP Tunnel types**.

d. Click .

e. Click **Close**.

f. Click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9.

7 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.

b. Select the rollover mode.

c. Click **Next**.

Result: The **User and Session Limits** window opens. See Figure 7-10.

8 Perform the following steps and click **Next**.

a. In the **User and Session Limits** section, select **No Limit**.

b. In the **Policy Limits** section, select **No Limit**.

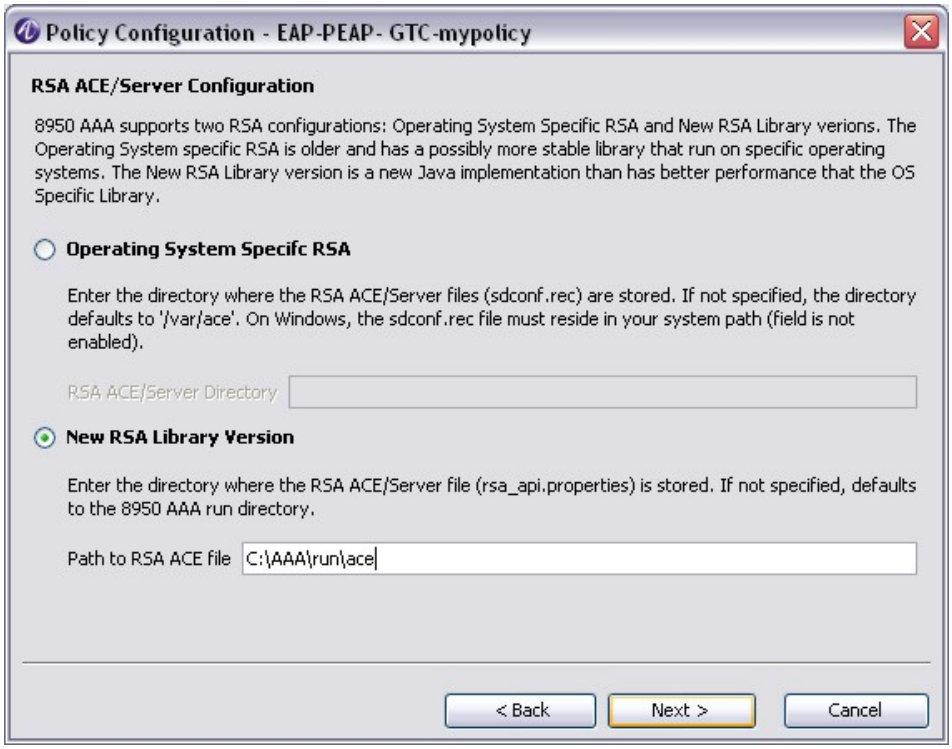
Result: The **RSA ACE/Server Configuration** window opens.

9 Perform the following steps.

a. Select **New RSA Library Version.**

b. Enter the path to the directory where the *RSA ACE\Server file\library* is stored.

Figure 7-22 RSA ACE/Server Configuration


Policy Configuration - EAP-PEAP- GTC-mypolicy
RSA ACE/Server Configuration
8950 AAA supports two RSA configurations: Operating System Specific RSA and New RSA Library verions. The Operating System specific RSA is older and has a possibly more stable library that run on specific operating systems. The New RSA Library version is a new Java implementation than has better performance that the OS Specific Library.
Operating System Specifc RSA
Enter the directory where the RSA ACE/Server files (sdconf.rec) are stored. If not specified, the directory defaults to '/var/ace'. On Windows, the sdconf.rec file must reside in your system path (field is not enabled).
RSA ACE/Server Directory
New RSA Library Version
Enter the directory where the RSA ACE/Server file (rsa_api.properties) is stored. If not specified, defaults to the 8950 AAA run directory.
Path to RSA ACE file
C:\AAA\run\ace
< Back
Next >
Cancel

c. Click **Next.**

Result: The **EAP PEAP GTC** configuration window opens. See Figure 7-17.

10 Perform the following steps and click **Next**.

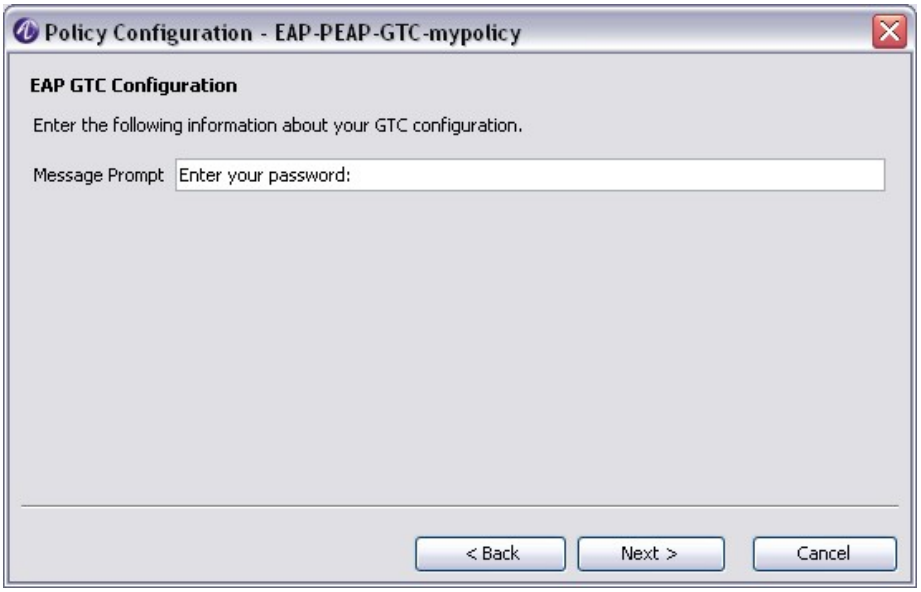
a. Enter the certificate file name and private key password for RSA or DSA.

b. Enter the challenge prompt.
c. Specify the compatibility mode for PEAP Version1.

Result: The **EAP GTC Configuration** window opens.

11 Enter the message prompt for GTC configuration.

Figure 7-23 EAP GTC configuration



Click **Next**.

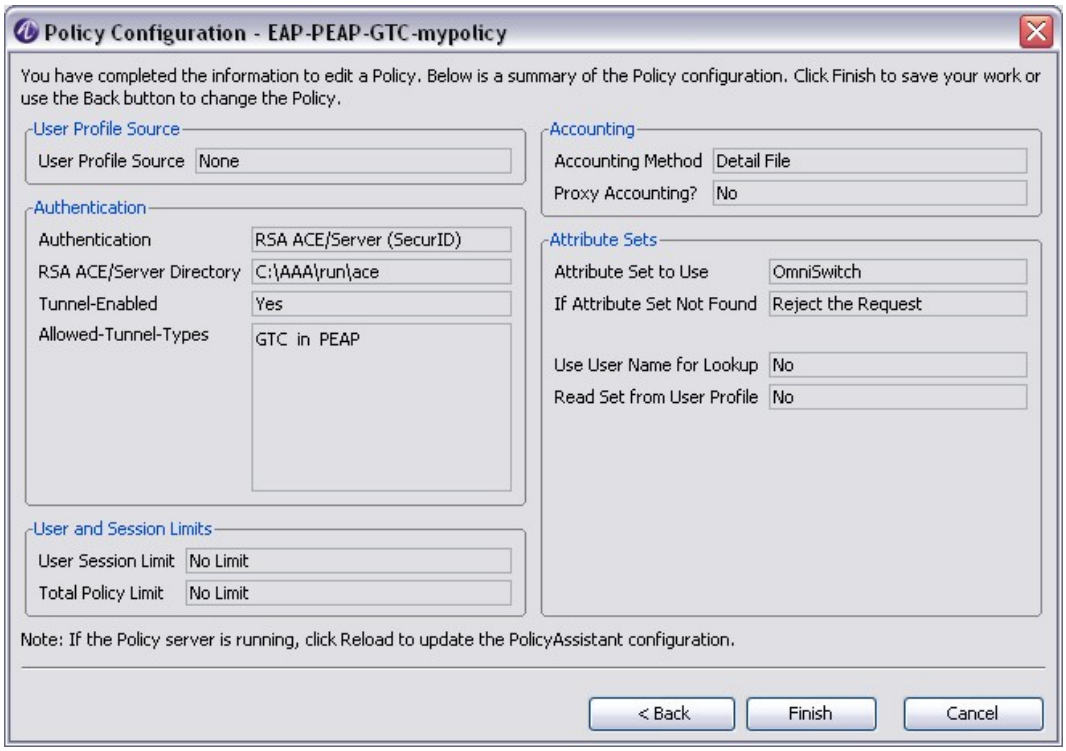
Result: The **Attribute Set for Policy** window opens. See Figure 7-12.

12 Perform the following steps:

a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.
b. From the list of templates, select **OmniSwitch**. For more information to configure templates, see Configure templates.
c. From the **Attribute Set Lookup Failure** section, select **Reject the Request**.
d. Click **Next**.

Result: A window with a summary of policy configuration opens.

Figure 7-24 Policy configuration summary


Policy Configuration - EAP-PEAP-GTC-mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source None
Authentication
Authentication RSA ACE/Server (SecurID)
RSA ACE/Server Directory C:\AAA\run\ace
Tunnel-Enabled Yes
Allowed-Tunnel-Types GTC in PEAP
User and Session Limits
User Session Limit No Limit
Total Policy Limit No Limit
Accounting
Accounting Method Detail File
Proxy Accounting? No
Attribute Sets
Attribute Set to Use OmniSwitch
If Attribute Set Not Found Reject the Request
Use User Name for Lookup No
Read Set from User Profile No
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

13 Click **Finish** to complete the PolicyAssistant configuration.

14 Click **Save** to save the policy created.

Configure EAP-PEAP-AD authentication

Purpose

Use this procedure to configure EAP-PEAP-AD using PolicyAssistant. Modify the configuration settings for local policies on a system running on Windows to allow EAP-PEAP-AD. For more details, see appendix, Machine authentication.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens. See Figure 7-5.

2 Click to add a new policy.

Result: The **Policy Configuration** window opens. See Figure 7-6.

3 Enter a new name for your policy. For example, enter the policy name as *EAP-PEAP-AD-mypolicy*. Click **Next**.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

4 Select **None** and click **Next.**

Result: The **Authenticating Access Requests** window opens. See Figure 7-8.

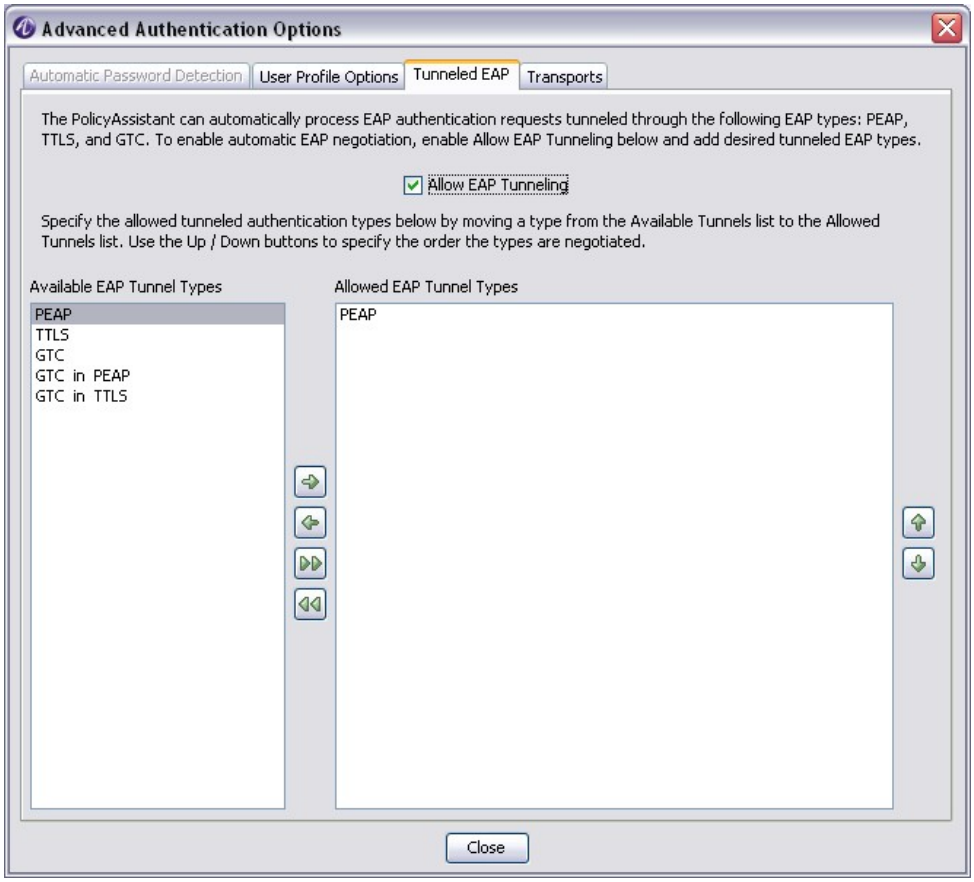
5 Perform the following steps:

a. Expand **EAP Authentication**.

b. Select **EAP MS Chap V2 (NT password).**

c. Click **Advanced Authentication Option.**

Figure 7-25 Advanced Authentication Options


Advanced Authentication Options
Automatic Password Detection
User Profile Options
Tunneled EAP
Transports
The PolicyAssistant can automatically process EAP authentication requests tunneled through the following EAP types: PEAP, TTLS, and GTC. To enable automatic EAP negotiation, enable Allow EAP Tunneling below and add desired tunneled EAP types.
Allow EAP Tunneling
Specify the allowed tunneled authentication types below by moving a type from the Available Tunnels list to the Allowed Tunnels list. Use the Up / Down buttons to specify the order the types are negotiated.
Available EAP Tunnel Types
PEAP
TTLS
GTC
GTC in PEAP
GTC in TTLS
Allowed EAP Tunnel Types
PEAP
Close

d. Select **User Profile Options** tab.

e. Select **Ignore Auth-Type attributes in the user profile**.

f. Select **EAP Tunneling** tab.

g. Select **PEAP** in **Allowed EAP Tunnel types**.

h. Click .

i. Click **Close**.

j. Click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9.

6 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.

b. Select the rollover mode.

c. Click **Next**.

Result: The **User and Session Limits** window opens. See Figure 7-10.

7 Perform the following steps and click **Next**.

a. In the **User and Session Limits** section, select **No Limit**.

b. In the **Policy Limits** section, select **No Limit**.

Result: The **EAP PEAP Configuration** window opens. See Figure 7-17.

8 Perform the following steps and click **Next**.

a. Enter the certificate file name and private key password for RSA or DSA.

b. Enter the challenge prompt.

c. Specify the compatibility mode for PEAP Version1.

Result: The **EAP MS CHAP V2 Authentication Configuration** window opens. See Figure 7-18.

9 Perform the following steps:

a. Enter the Windows domain or computer name on which the Microsoft Windows SAM server is running. Enter the domain or computer name only if EAP MS Chap V2 (NT Password) is chosen.

b. Select **EAP client uses user instead of user@realm to generate challenges**.

c. Click **Next**.

Result: The **CRL (Certificate Revocation List) Configuration** window opens. See Figure 7-19.

10 Click **Next**.

Result: The **Attribute Set for Policy** window opens. See Figure 7-12.

11 Perform the following steps:

a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.

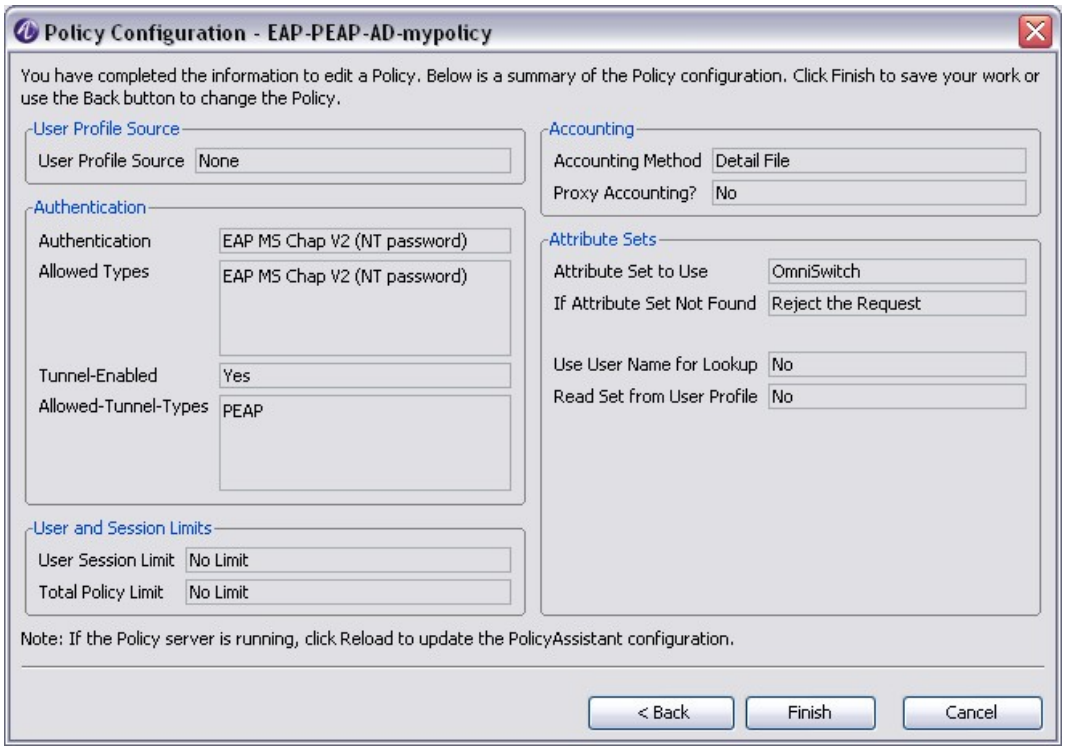
b. From the list of templates, select **OmniSwitch**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failure** section, select **Reject the Request**.

d. Click **Next**.

Result: A window with a summary of policy configuration opens.

Figure 7-26 Policy configuration summary


Policy Configuration - EAP-PEAP-AD-mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source None
Authentication
Authentication EAP MS Chap V2 (NT password)
Allowed Types EAP MS Chap V2 (NT password)
Tunnel-Enabled Yes
Allowed-Tunnel-Types PEAP
User and Session Limits
User Session Limit No Limit
Total Policy Limit No Limit
Accounting
Accounting Method Detail File
Proxy Accounting? No
Attribute Sets
Attribute Set to Use OmniSwitch
If Attribute Set Not Found Reject the Request
Use User Name for Lookup No
Read Set from User Profile No
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

12 Click **Finish** to complete the PolicyAssistant configuration.

13 Click **Save** to save the policy created.

Configure EAP-TLS authentication with RADIUS User File as user source

Use this procedure to configure EAP-TLS authentication using PolicyAssistant. Users are authenticated using X.509 certificates. This authentication method does not involve any user credential authentication.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens.

2 Click to add a new policy.

Result: The **Policy Configuration** window opens. See Figure 7-6.

3 Enter a new name for your policy. For example, enter the policy name as *EAP-TLS-mypolicy*. Click **Next**.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

4 Select **None** and click **Next**.

Result: The **Authentication Access Requests** window opens. See Figure 7-8.

5 Expand **EAP Authentication** in the list of **Authentication Types**, select **EAP TLS** and click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9.

6 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.

b. Select the rollover mode.

c. Click **Next**.

Result: The **User and Session Limits** window opens. See Figure 7-10.

7 Perform the following steps and click **Next**.

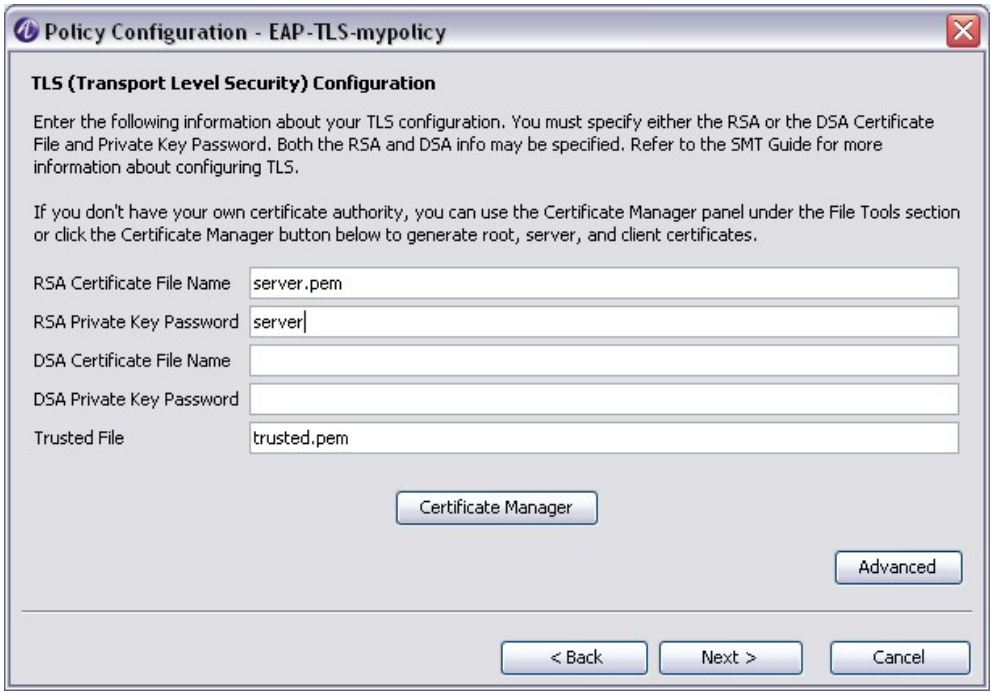
a. In the **User Session Limits** section, select **No Limit**.

b. In the **Policy Limits** section, select **No Limit**.

Result: The **TLS (Transport Level Security) Configuration** window opens.

8 Enter the certificate file name and private key password for RSA or DSA.

Figure 7-27 TLS (Transport Level Security) Configuration


Policy Configuration - EAP-TLS-mypolicy
TLS (Transport Level Security) Configuration
Enter the following information about your TLS configuration. You must specify either the RSA or the DSA Certificate File and Private Key Password. Both the RSA and DSA info may be specified. Refer to the SMT Guide for more information about configuring TLS.
If you don't have your own certificate authority, you can use the Certificate Manager panel under the File Tools section or click the Certificate Manager button below to generate root, server, and client certificates.
RSA Certificate File Name
server.pem
RSA Private Key Password
server
DSA Certificate File Name
DSA Private Key Password
Trusted File
trusted.pem
Certificate Manager
Advanced
< Back
Next >
Cancel

9 Click **Next**.

Result: The **CRL (Certificate Revocation List) Configuration** window opens. See Figure 7-19.

10 Check **CRL Checking Enabled** and enter the certificate file name in **CRL Issuer Certificate File**. Click **Next**.

Result: The **Attribute Set for Policy** window opens. See Figure 7-12.

11 Perform the following steps and click **Next**.

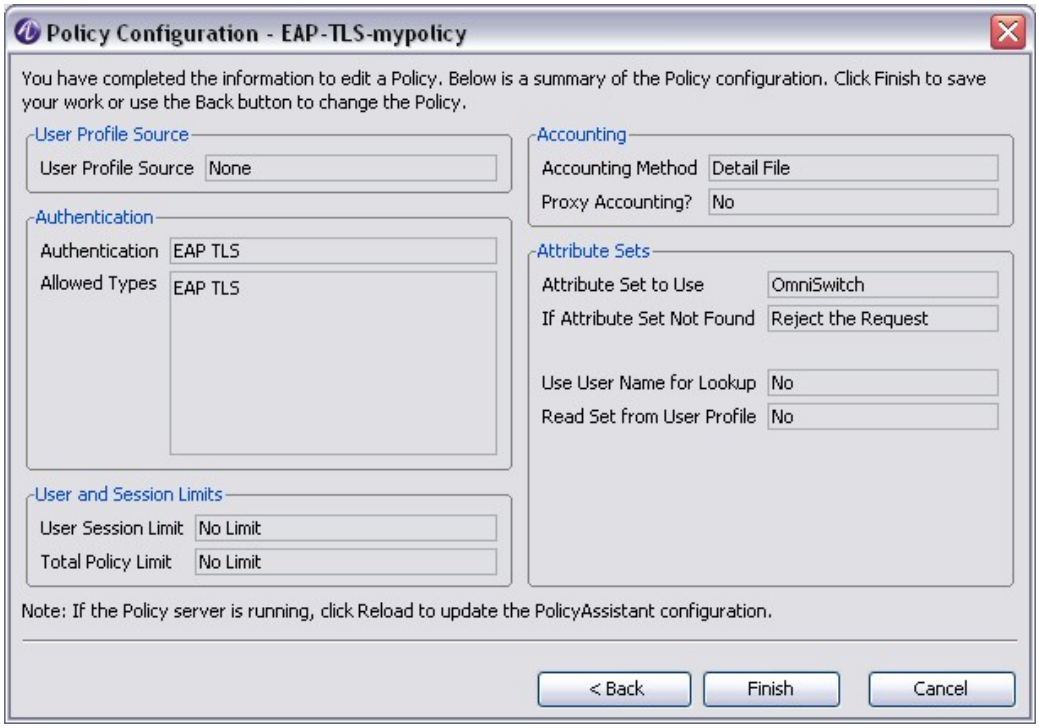
a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.

b. From the list of templates, select **OmniSwitch**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failure** section, select **Reject the Request**.

Result: A window with a summary of policy configuration opens.

Figure 7-28 Policy configuration summary


Policy Configuration - EAP-TLS-mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source None
Authentication
Authentication EAP TLS
Allowed Types EAP TLS
User and Session Limits
User Session Limit No Limit
Total Policy Limit No Limit
Accounting
Accounting Method Detail File
Proxy Accounting? No
Attribute Sets
Attribute Set to Use OmniSwitch
If Attribute Set Not Found Reject the Request
Use User Name for Lookup No
Read Set from User Profile No
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

12 Click **Finish** to complete the PolicyAssistant configuration.

13 Click **Save** to save the policy created.

Configure EAP-TTLS-MS-Chapv2 authentication with RADIUS User File as user source

Purpose

Use this procedure to configure EAP-TTLS (EAP-MSChapV2 as inner authentication and no CRL checking) authentication with RADIUS user file as user source using PolicyAssistant. Users are authenticated inside a secure tunnel.

Procedure

1. From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

   Result: The **PolicyAssistant** window opens.

2. Click to add a new policy.

   Result: The **Policy Configuration** window opens. See Figure 7-6.

3. Enter a new name for your policy. For example, enter the policy name as *EAP-TTLS-mypolicy*. Click **Next**.

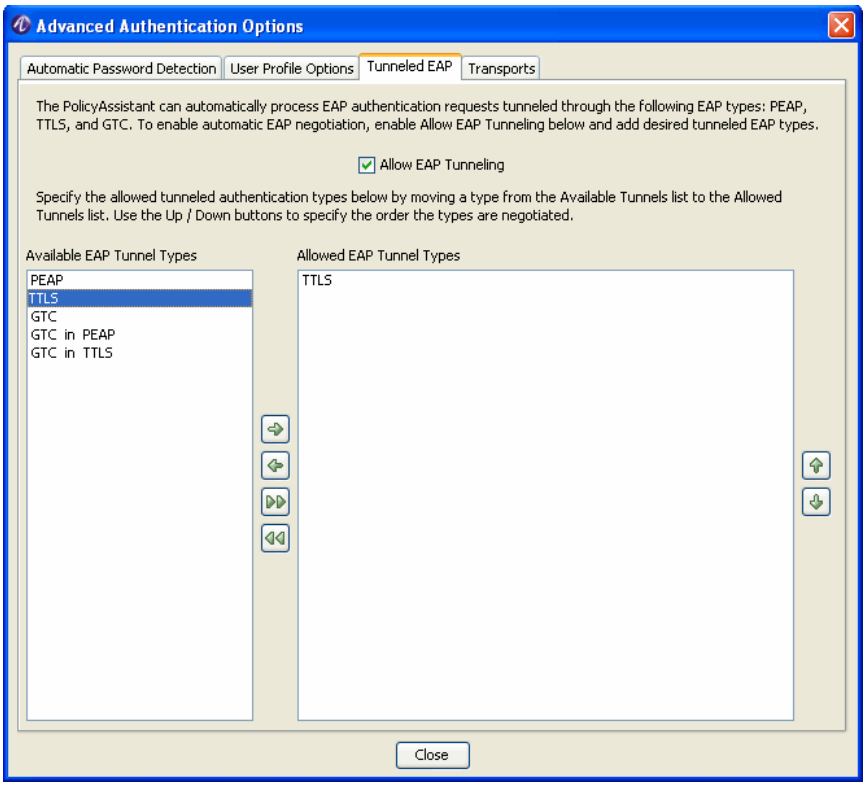
   Result: The **Source for User Profiles** window opens. See Figure 7-7.

4. Select **RADIUS User File** and click **Next**.

   Result: The **Authentication Access Requests** window opens. See Figure 7-8.

5. Perform the following steps:
   a. Expand **EAP Authentication** in the list of **Authentication Types** and select **EAP MS Chap V2**.
   b. Click **Advanced Authentication Options** tab.
   c. In the **Advanced Authentication Options** window, select **Tunneled EAP** tab.
   d. Select **Allow EAP Tunneling**.
   e. From the **Available EAP Tunnel Types** section, select **TTLS** and click . See Figure 7-29.

Figure 7-29 Advanced Authentication Options


Advanced Authentication Options
Automatic Password Detection
User Profile Options
Tunneled EAP
Transports
The PolicyAssistant can automatically process EAP authentication requests tunneled through the following EAP types: PEAP, TTLS, and GTC. To enable automatic EAP negotiation, enable Allow EAP Tunneling below and add desired tunneled EAP types.
Allow EAP Tunneling
Specify the allowed tunneled authentication types below by moving a type from the Available Tunnels list to the Allowed Tunnels list. Use the Up / Down buttons to specify the order the types are negotiated.
Available EAP Tunnel Types
PEAP
TTLS
GTC
GTC in PEAP
GTC in TTLS
Allowed EAP Tunnel Types
TTLS
Close

f. Click **Close**.

g. Click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9.

6 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.

b. Select the rollover mode.

c. Click N**ext**.

Result: The **User and Session Limits** window opens. See Figure 7-10.

7 Perform the following steps:

a. In the **User Session Limits** section, select **No Limit**.

b. In the **Policy Limits** section, select **No Limit**.

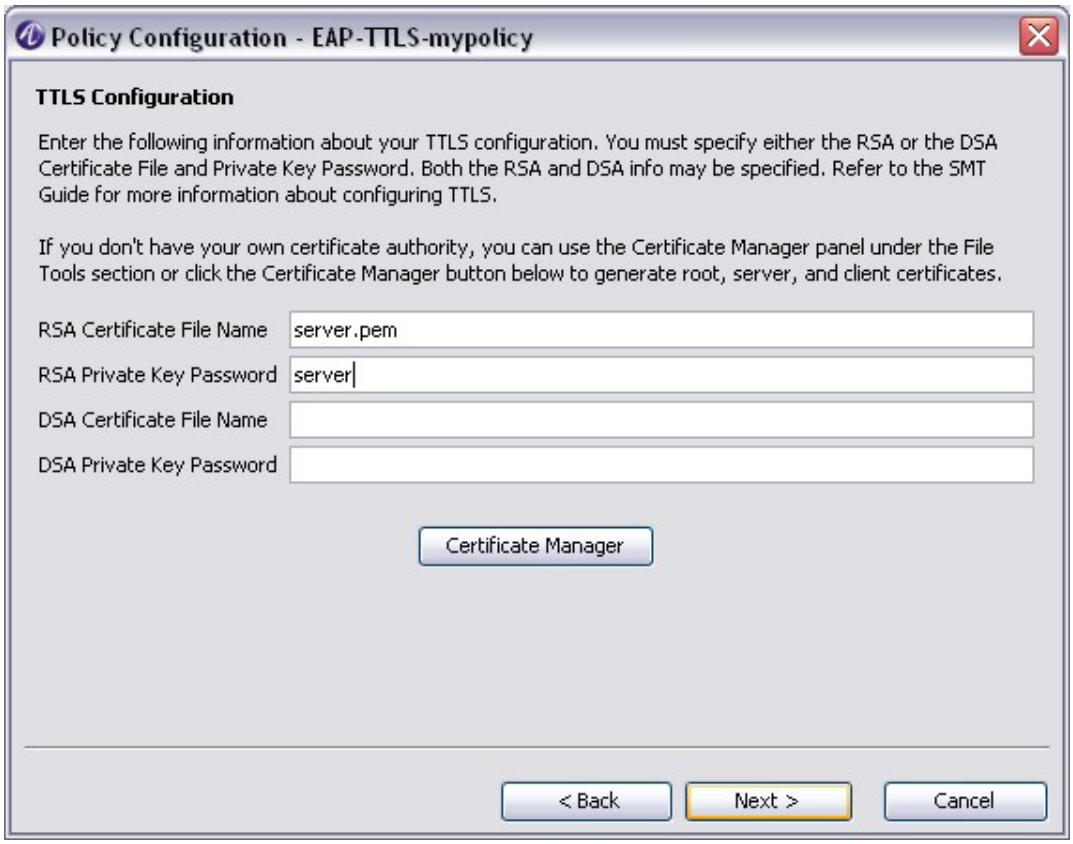
c. Click **Next**.

Result: The **User File Name Configuration** window opens. See Figure 7-14.

8 The user file name appears by default. If needed, modify the user file name and click **Next**.

Result: The **EAP-TTLS Configuration** window opens.

Figure 7-30 EAP TTLS Configuration


Policy Configuration - EAP-TTLS-mypolicy
TTLS Configuration
Enter the following information about your TTLS configuration. You must specify either the RSA or the DSA Certificate File and Private Key Password. Both the RSA and DSA info may be specified. Refer to the SMT Guide for more information about configuring TTLS.
If you don't have your own certificate authority, you can use the Certificate Manager panel under the File Tools section or click the Certificate Manager button below to generate root, server, and client certificates.
RSA Certificate File Name
server.pem
RSA Private Key Password
server
DSA Certificate File Name
DSA Private Key Password
Certificate Manager
< Back
Next >
Cancel

9 Enter the certificate file name and private key password for RSA or DSA. Click **Next**.

Result: The **EAP MS CHAP V2 Authentication Configuration** window opens.

10 Perform the following steps and click **Next**.

a. Enter the Windows domain name or computer name on which the Microsoft Windows SAM server is running. Enter the domain or computer name only if EAP MS Chap V2 (NT Password) is chosen.

b. Select **EAP client uses user instead of user@realm to generate challenges**.

Result: The **CRL (Certificate Revocation List) Configuration** window opens.

11 Click **Next**.

Result: The **Attribute Set for Policy** window opens. See Figure 7-12.

12 Perform the following steps and click **Next.**

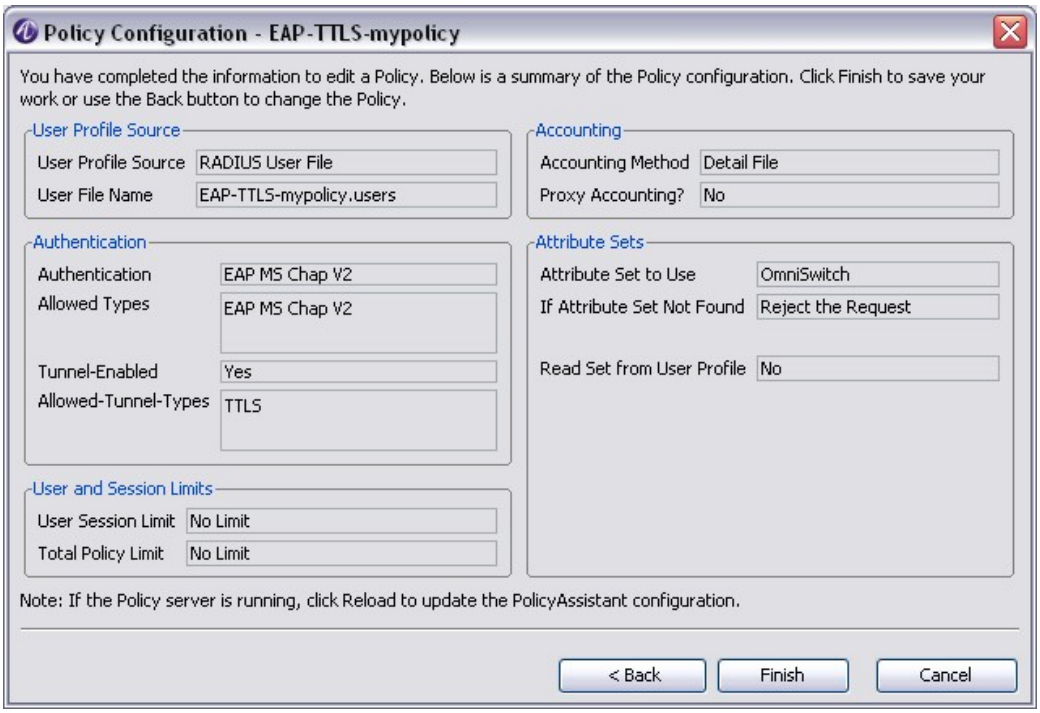
a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.

b. From the list of templates, select **OmniSwitch**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failure** section, select **Reject the Request**.

Result: A window with a summary of policy configuration opens.

Figure 7-31 Policy configuration summary


Policy Configuration - EAP-TTLS-mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source RADIUS User File
User File Name EAP-TTLS-mypolicy.users
Accounting
Accounting Method Detail File
Proxy Accounting? No
Authentication
Authentication EAP MS Chap V2
Allowed Types EAP MS Chap V2
Tunnel-Enabled Yes
Allowed-Tunnel-Types TTLS
Attribute Sets
Attribute Set to Use OmniSwitch
If Attribute Set Not Found Reject the Request
Read Set from User Profile No
User and Session Limits
User Session Limit No Limit
Total Policy Limit No Limit
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

13 Click **Finish** to complete the PolicyAssistant configuration.

14 Click **Save** to save the policy created.

Configure authentication with Microsoft Active Directory as user source

Purpose

Use this procedure to configure authentication with user source as Microsoft Active Directory using PolicyAssistant.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens. See Figure 7-6.

2 Enter a new name for your policy. For example, enter the policy name as *AuthWindowsAD-mypolicy*. Click **Next**.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

3 Select **Microsoft Active Directory** and click **Next**.

Result: The **Authenticating Access Requests** window opens. See Figure 7-8.

4 Expand **External Authentications,** select **Microsoft Active Directory** and click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9.

5 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.

b. Select the rollover mode.

c. Click N**ext**.

Result: The **User and Session Limits** window opens. See Figure 7-10.

6 Perform the following:

In the **User Session Limits** section, select **No Limit**.

a. In the **Policy Limits section**, select **No Limit**.

b. Click **Next**.

Result: The **Microsoft Active Directory Configuration** window opens.

7 Perform the following:

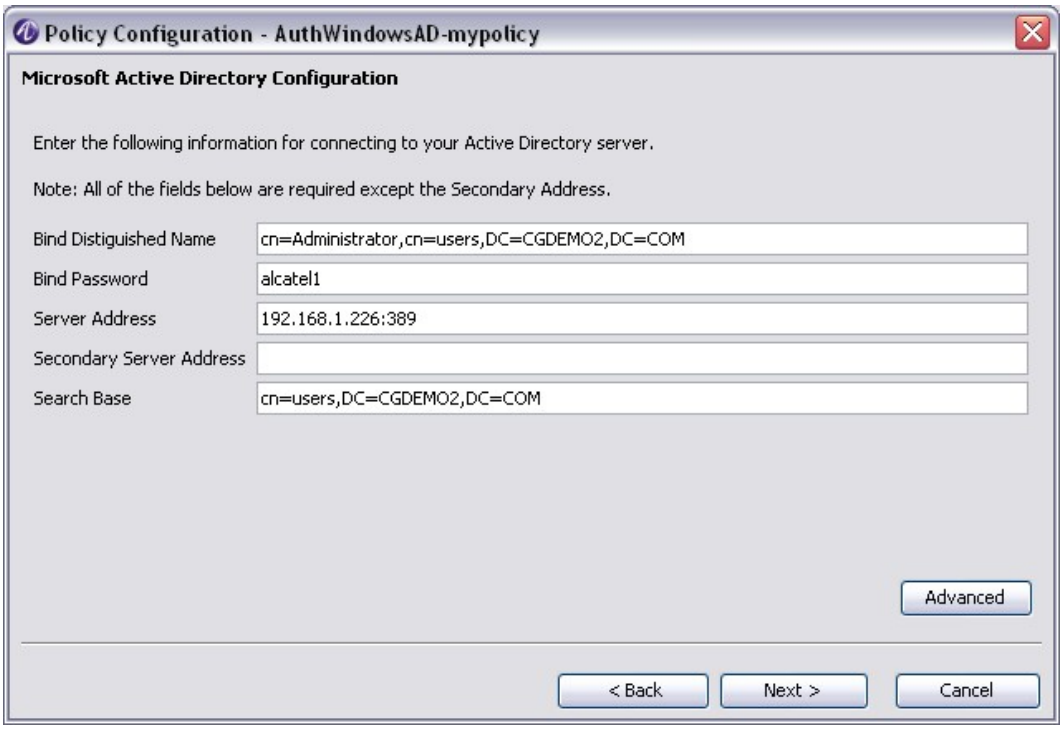
a. Enter the Bind Distinguished Name.

b. Enter the Bind Password.

c. Enter the Server Address.

d. Enter the Search Base.

Figure 7-32 Microsoft Active Directory Configuration



e. Click **Next**.

Result: The **Attribute Set for Policy** window opens. See Figure 7-12.

8 Perform the following:

a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.

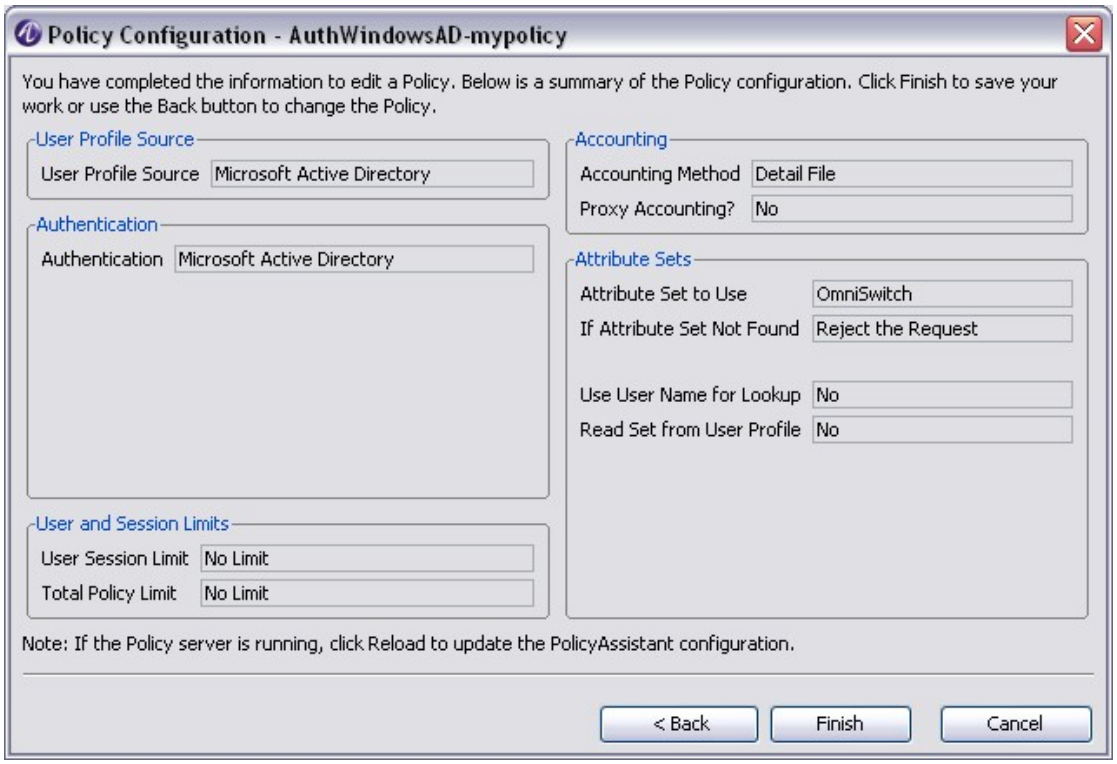
b. From the list of templates, select **OmniSwitch**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failure** section, select **Reject the Request**.

d. Click **Next**.

Result: A window with a summary of policy configuration opens.

Figure 7-33 Policy configuration summary


Policy Configuration - AuthWindowsAD-mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source Microsoft Active Directory
Authentication
Authentication Microsoft Active Directory
User and Session Limits
User Session Limit No Limit
Total Policy Limit No Limit
Accounting
Accounting Method Detail File
Proxy Accounting? No
Attribute Sets
Attribute Set to Use OmniSwitch
If Attribute Set Not Found Reject the Request
Use User Name for Lookup No
Read Set from User Profile No
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

9 Click **Finish** to complete the PolicyAssistant configuration.

10 Click **Save** to save the policy created.

Configure SAM authentication

Purpose

Use this procedure to configure Windows SAM authentication with user source as RADIUS User file using PolicyAssistant.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens. See Figure 7-6.

2 Enter a new name for your policy. For example, enter the policy name as *AuthWindowsSAM-mypolicy*. Click **Next**.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

3 Select **Windows Security Access Manager** and click **Next**.

Result: The **Authenticating Access Requests** window opens. See Figure 7-8.

4 Expand **External Authentications,** select **Windows Security Access Manager** and click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9.

5 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.
b. Select the rollover mode.
c. Click N**ext**.

Result: The **User and Session Limits** window opens. See Figure 7-10.

6 Perform the following:

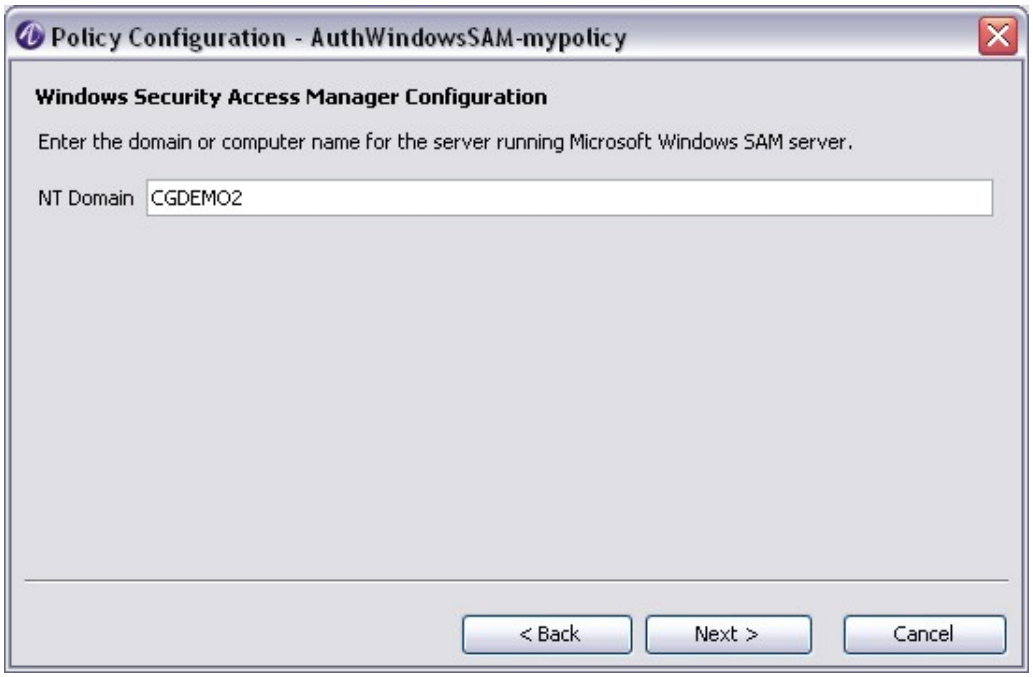
a. In the **User Session Limits** section, select **No Limit**.
b. In the **Policy Limits** section, select **No Limit**.
c. Click **Next**.

Result: The **User File Name Configuration** window opens. See Figure 7-14.

7 Enter the user file name and click **Next.**

Result: The **Windows Security Access Manager Configuration** window opens. See Figure 7-34.

Figure 7-34 Windows Security Access Manager


Policy Configuration - AuthWindowsSAM-mypolicy
Windows Security Access Manager Configuration
Enter the domain or computer name for the server running Microsoft Windows SAM server.
NT Domain
CGDEMO2
< Back
Next >
Cancel

8 Enter the domain or computer name on which the Windows Security Access Manager is running. Click **Next**.

Result: The **Attribute Set for Policy** window opens. See Figure 7-12.

9 Perform the following:

a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.

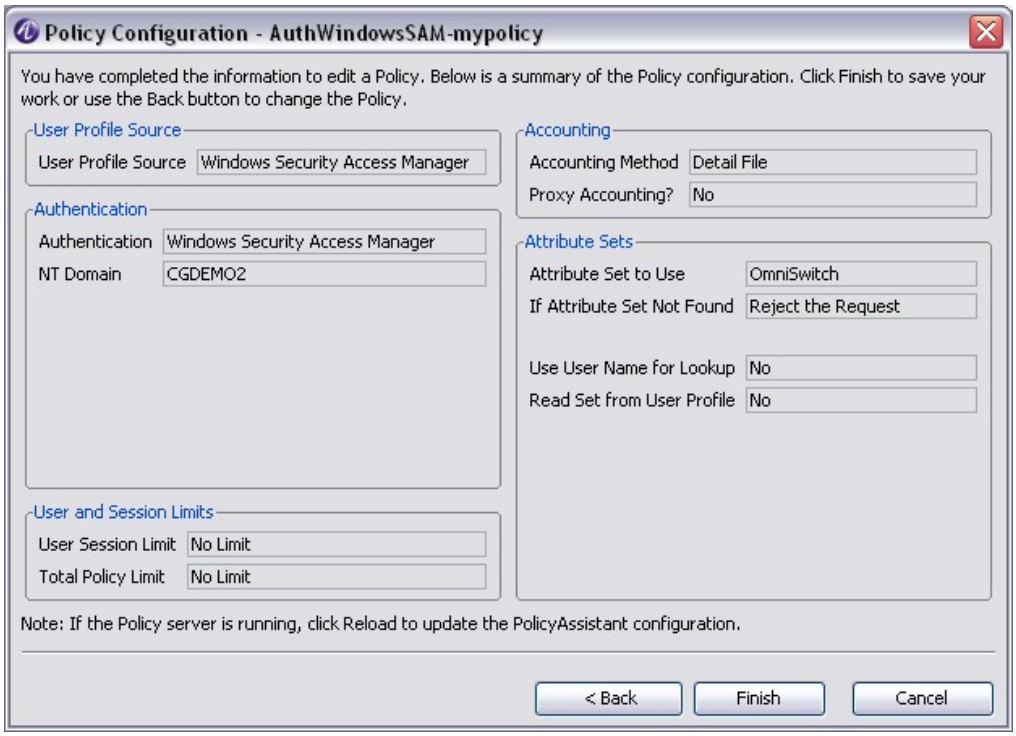
b. From the list of templates, select **OmniSwitch**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failure** section, select **Reject the Request**.

d. Click **Next**.

Result: A window with a summary of policy configuration opens.

Figure 7-35 Policy configuration summary


Policy Configuration - AuthWindowsSAM-mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source Windows Security Access Manager
Authentication
Authentication Windows Security Access Manager
NT Domain CGDEMO2
User and Session Limits
User Session Limit No Limit
Total Policy Limit No Limit
Accounting
Accounting Method Detail File
Proxy Accounting? No
Attribute Sets
Attribute Set to Use OmniSwitch
If Attribute Set Not Found Reject the Request
Use User Name for Lookup No
Read Set from User Profile No
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

10 Click **Finish** to complete the PolicyAssistant configuration.

11 Click **Save** to save the policy created.

Configure RSA/ACE server as a user source for secureID tokens

Purpose

Use this procedure to authenticate users against RSA/ACE server as a user source for secureID tokens using PolicyAssistant.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens.

2 Click to add a new policy.

Result: The **Policy Configuration** window opens. See Figure 7-6.

3 Enter a new name for your policy. For example, enter the policy name as *RSA-mypolicy*. Click **Next**.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

4 Select **RSA ACE/Server (SecureID)** and click **Next.**

Result: The **Accounting Configuration** window opens. See Figure 7-9.

5 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.

b. Select the rollover mode.

c. Click **Next**.

Result: The **User and Session Limits** window opens. See Figure 7-10.

6 Perform the following steps:

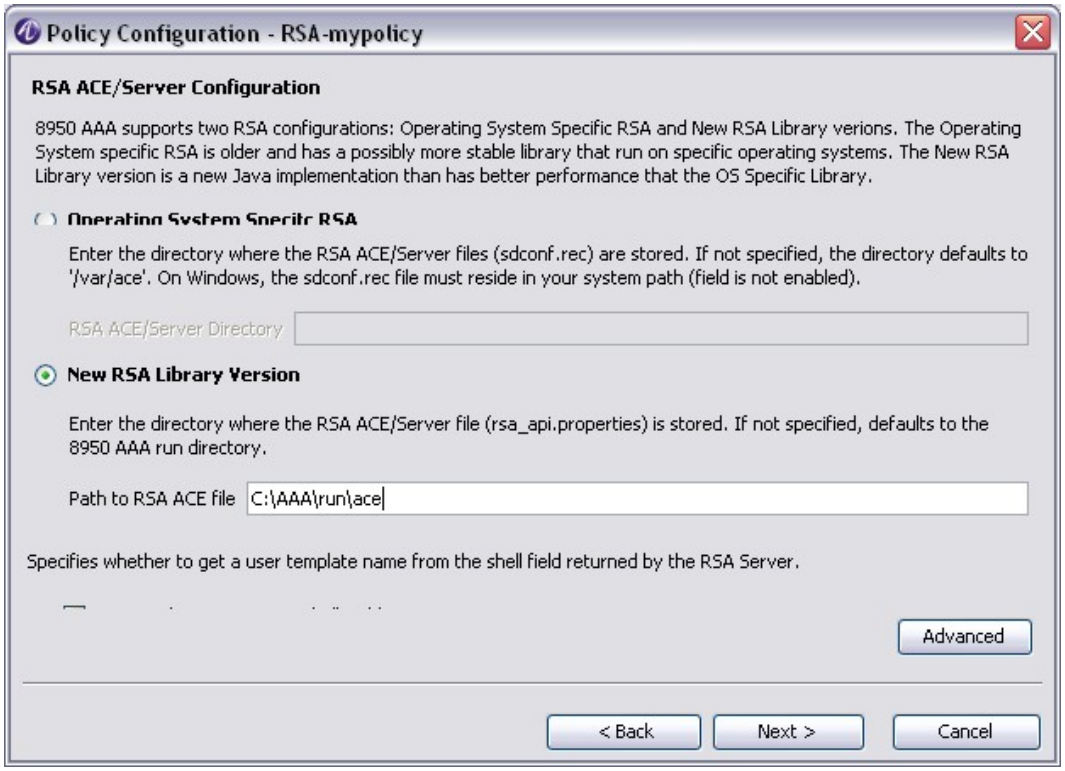
a. In the **User Session Limits** section, select **No Limit**.

b. In the **Policy Limits** section, select **No Limit**.

c. Click **Next**.

Result: The **RSA ACE/Server Configuration** window opens.

Figure 7-36 RSA ACE/Server Configuration


Policy Configuration - RSA-mypolicy
RSA ACE/Server Configuration
8950 AAA supports two RSA configurations: Operating System Specific RSA and New RSA Library verions. The Operating System specific RSA is older and has a possibly more stable library that run on specific operating systems. The New RSA Library version is a new Java implementation than has better performance that the OS Specific Library.
Operating System Specific RSA
Enter the directory where the RSA ACE/Server files (sdconf.rec) are stored. If not specified, the directory defaults to '/var/ace'. On Windows, the sdconf.rec file must reside in your system path (field is not enabled).
RSA ACE/Server Directory
New RSA Library Version
Enter the directory where the RSA ACE/Server file (rsa_api.properties) is stored. If not specified, defaults to the 8950 AAA run directory.
Path to RSA ACE file
C:\AAA\run\ace
Specifies whether to get a user template name from the shell field returned by the RSA Server.
Advanced
< Back
Next >
Cancel

7 Perform the following steps:

a. Select **New RSA Library Version**.

b. Enter the path to the directory where the *RSA ACE\Server file\library* is stored.

c. Click **Next**.

Result: The **Attribute Set for Policy** window opens. See Figure 7-12.

8 Perform the following steps:

a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.

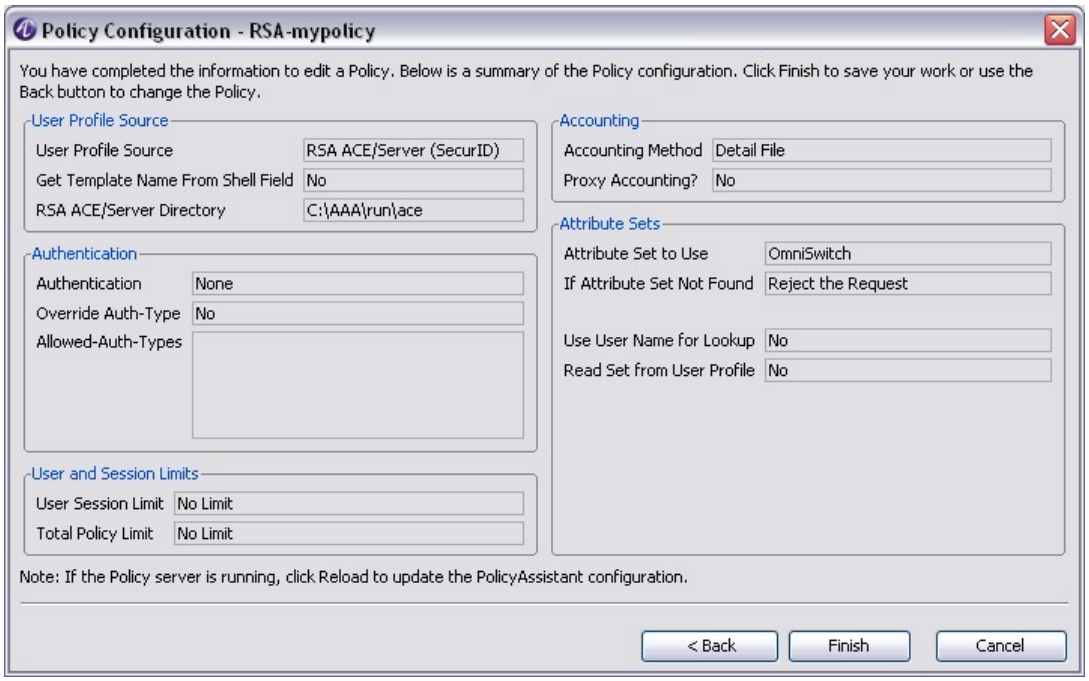
b. From the list of templates, select **OmniSwitch**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failure** section, select **Reject the Request**.

d. Click **Next**.

Result: A window with a summary of policy configuration opens.

Figure 7-37 Policy configuration summary



9 Click **Finish** to complete the PolicyAssistant configuration.

10 Click **Save** to save the policy created.

Configure proxy authentication for RADIUS server

Purpose

Use this procedure to proxy authentication and accounting requests from RADIUS server.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens. See Figure 7-5.

2 Click to add a new policy.

Result: The **Policy Configuration** window opens. See Figure 7-6.

3 Enter a new name for your policy. For example, enter the policy name as *proxy- mypolicy*. Click **Next**.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

4 Select **Radius Server (Proxy)** and click **Next**.

Result: The **Authentication Access Requests** window opens. See Figure 7-8.

5 Expand **EAP Authentication** in the list of **Authentication Types**, select **EAP MD5** and click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9.

6 Perform the following steps and Click **Next**:

a. Select **Discard Accounting Information**.

b. Select **Proxy Accounting Information** checkbox.

Result: The **User and Session Limits** window opens. See Figure 7-10.

7 Perform the following steps:

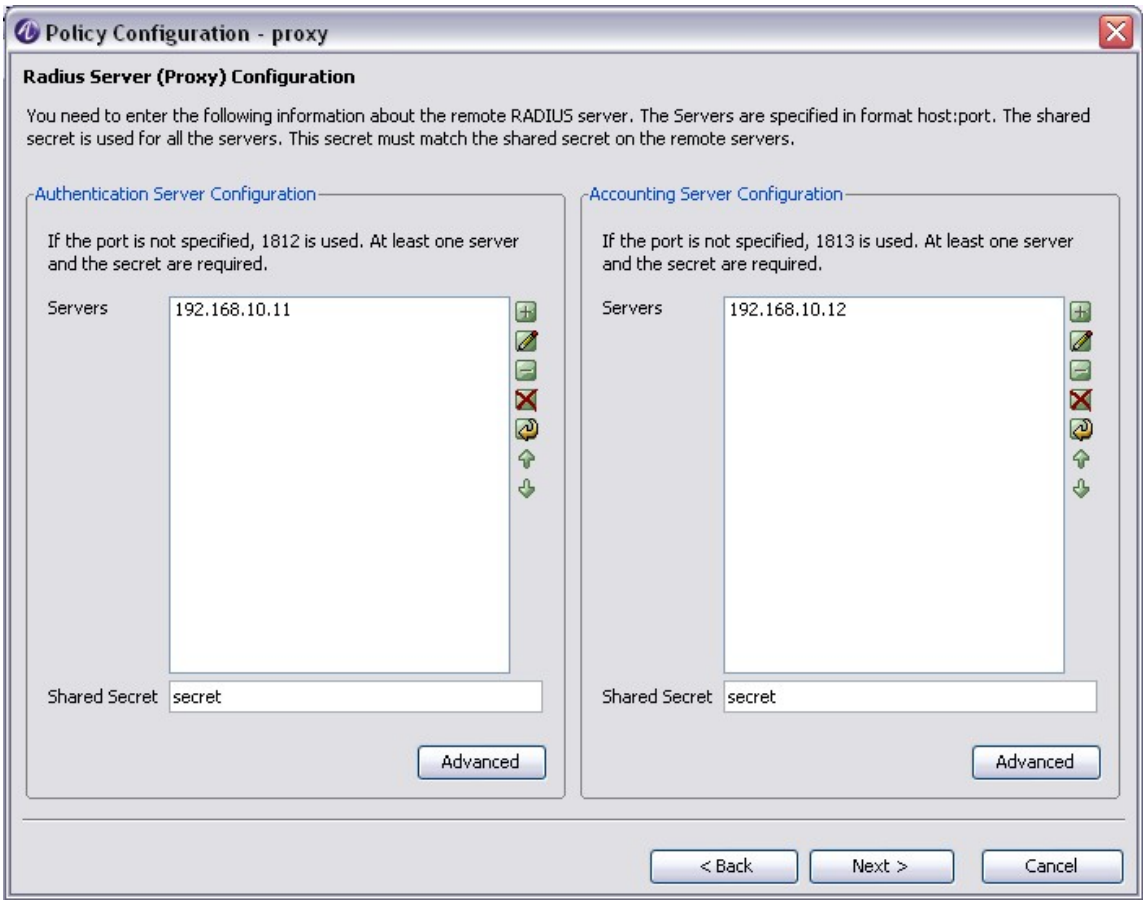
a. In the **User Session Limits** section, select **No Limit**.

b. In the **Policy Limits** section, select **No Limit**.

c. Click **Next**.

Result: The **Radius Server (Proxy) Configuration** window opens.

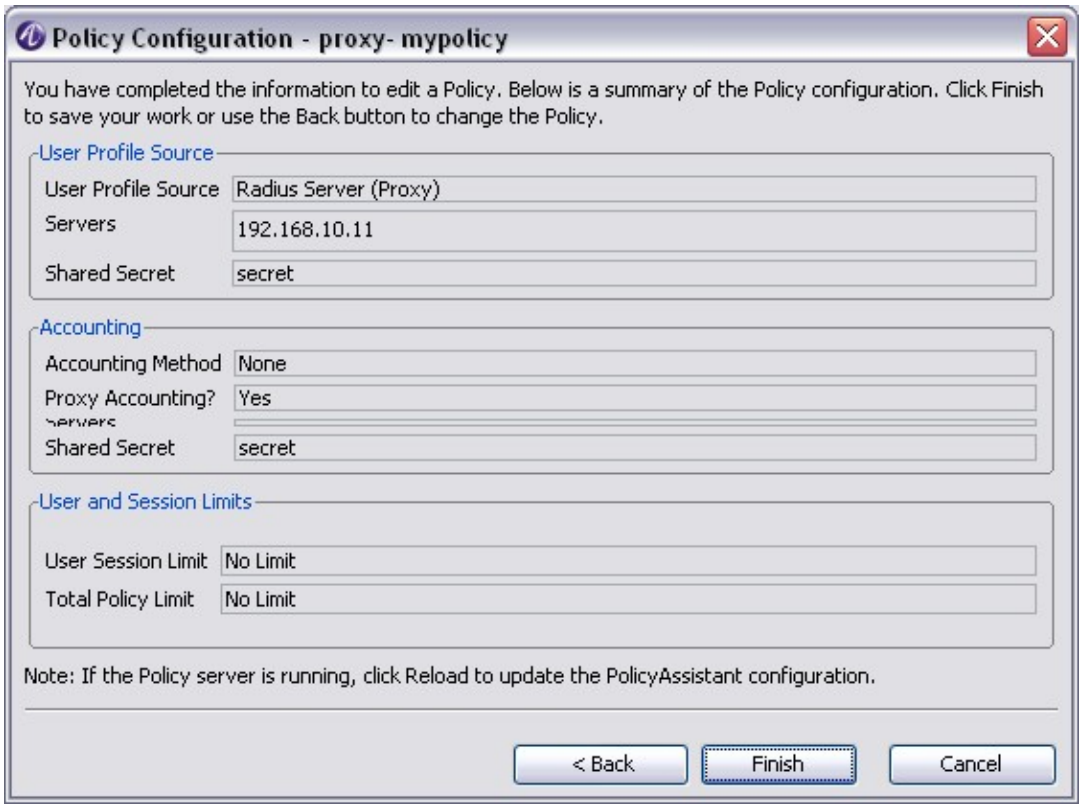
Figure 7-38 Radius Server (Proxy) Configuration


Policy Configuration - proxy
Radius Server (Proxy) Configuration
You need to enter the following information about the remote RADIUS server. The Servers are specified in format host:port. The shared secret is used for all the servers. This secret must match the shared secret on the remote servers.
Authentication Server Configuration
If the port is not specified, 1812 is used. At least one server and the secret are required.
Servers
192.168.10.11
Shared Secret
secret
Advanced
Accounting Server Configuration
If the port is not specified, 1813 is used. At least one server and the secret are required.
Servers
192.168.10.12
Shared Secret
secret
Advanced
< Back
Next >
Cancel

8 Enter the proxy port address for both authentication server and the accounting server and click **Next**.

Result: A window with a summary of policy configuration opens.

Figure 7-39 Policy configuration summary



9 Click **Finish** to complete the PolicyAssistant configuration for proxy RADIUS server.

10 Click **Save** to save the policy created.

Configure PolicyAssistant rules for CyberGateKeeper

This section contains procedures to configure PolicyAssistant for different samples of CyberGateKeeper.

Note: Samples are provided for the following three different audit categories of the CyberGateKeeper.

- Pass-Audit
- Fail-Audit
- Fail-Noaudit

Configure CG-pass-MD5 authentication with RADIUS User File as user source for Pass Audit

Purpose

Use this procedure to configure CG -pass-MD5 authentication with the RADIUS User File as user source and using the PolicyAssistant. This sample policy is for Pass Audit status.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant.**

Result: The **PolicyAssistant** window opens.

2 Click to add a new policy.

Result: The **Policy Configuration** window opens. See Figure 7-6.

3 Enter a new name for your policy. For example, enter the policy name as *CG-pass-MD5-mypolicy*. Click **Next**.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

4 Select **Radius User File** and click **Next**.

Result: The **Authentication Access Requests** window opens. See Figure 7-8.

5 Expand **EAP Authentication** in the list of **Authentication Types**, select **EAP MD5** and click **Next.**

Result: The **Accounting Configuration** window opens. See Figure 7-9.

6 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.

b. Select the rollover mode.

c. Click **Next**.

Result: The **User and Session Limits** window opens. See Figure 7-10.

7 Perform the following steps:

a. In the **User and Session Limits** section, select **One Session**.

b. In the **Policy Limits** section, select **No Limit**.

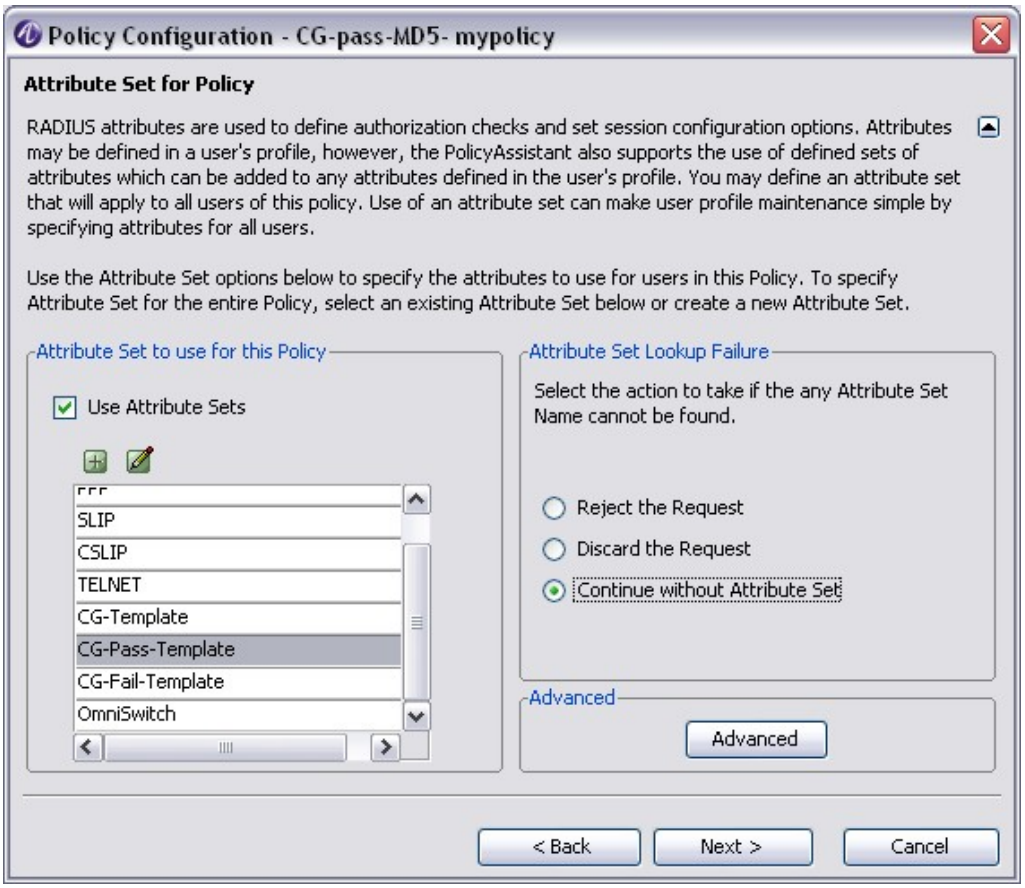
c. Click **Next**.

Result: The **User File Name Configuration** window opens. See Figure 7-14.

8 The user file name appears by default. If needed, modify the user file name and click **Next.**

Result: The **Attribute Set for Policy** window opens.

Figure 7-40 Attribute Set for Policy


Policy Configuration - CG-pass-MD5- mypolicy
Attribute Set for Policy
RADIUS attributes are used to define authorization checks and set session configuration options. Attributes may be defined in a user's profile, however, the PolicyAssistant also supports the use of defined sets of attributes which can be added to any attributes defined in the user's profile. You may define an attribute set that will apply to all users of this policy. Use of an attribute set can make user profile maintenance simple by specifying attributes for all users.
Use the Attribute Set options below to specify the attributes to use for users in this Policy. To specify Attribute Set for the entire Policy, select an existing Attribute Set below or create a new Attribute Set.
Attribute Set to use for this Policy
Use Attribute Sets
SLIP
CSLIP
TELNET
CG-Template
CG-Pass-Template
CG-Fail-Template
OmniSwitch
Attribute Set Lookup Failure
Select the action to take if the any Attribute Set Name cannot be found.
Reject the Request
Discard the Request
Continue without Attribute Set
Advanced
Advanced
< Back
Next >
Cancel

9 Perform the following steps:

a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.

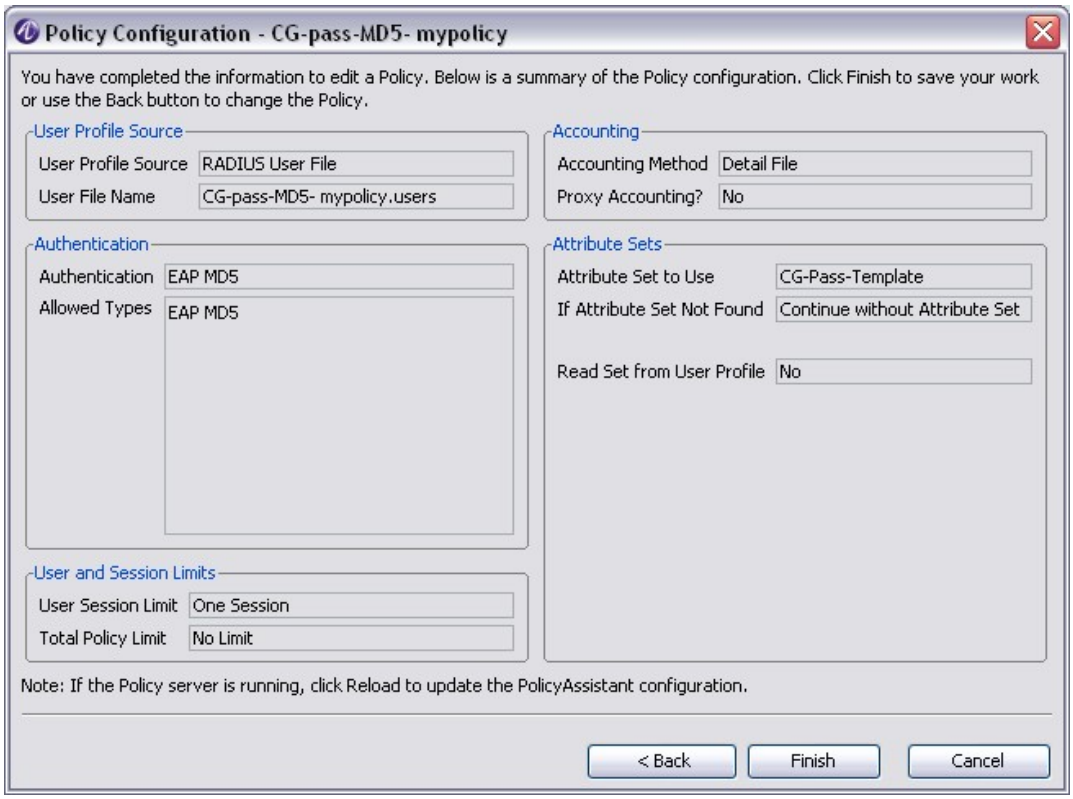
b. From the list of templates, select **CG-Pass-Template**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failur**e section, select **Continue without Attribute Set**.

d. Click **Next**.

Result: A window with a summary of policy configuration opens.

Figure 7-41 Policy configuration summary


Policy Configuration - CG-pass-MD5- mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source RADIUS User File
User File Name CG-pass-MD5- mypolicy.users
Accounting
Accounting Method Detail File
Proxy Accounting? No
Authentication
Authentication EAP MD5
Allowed Types EAP MD5
Attribute Sets
Attribute Set to Use CG-Pass-Template
If Attribute Set Not Found Continue without Attribute Set
Read Set from User Profile No
User and Session Limits
User Session Limit One Session
Total Policy Limit No Limit
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

10 Click **Finish** to complete the PolicyAssistant configuration for CG-pass-MD5.

11 Click **Save** to save the policy created.

Configure CG-fail-MD5 authentication with RADIUS User File as user source for Fail Audit

Purpose

Use this procedure to configure CG -fail-MD5 authentication with the RADIUS User File as user source and using the PolicyAssistant. This sample policy is for Fail Audit status.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens.

2 Click to add a new policy.

Result: The **Policy Configuration** window opens. See Figure 7-6.

3 Enter a new name for your policy. For example, enter the policy name as *CG-fail-MD5-mypolicy*. Click **Next**.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

4 Select **Radius User File** and click **Next**.

Result: The **Authentication Access Requests** window opens. See Figure 7-8.

5 Expand **EAP Authentication** in the list of **Authentication Types**, select **EAP-MD5** and click **Next**.

Result: The **Authenticating Access Requests** window opens. See Figure 7-8.

6 Select **EAP MD5** and click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9.

7 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.

b. Select the rollover mode.

c. Click **Next**.

Result: The **User and Session Limits** window opens. See Figure 7-10.

8 Perform the following steps:

a. In the **User and Session Limits** section, select **One Session**.

b. In the **Policy Limits** section, select **No Limit**.

c. Click **Next**.

Result: The **User File Name Configuration** window opens. See Figure 7-14.

9 The user file name appears by default. If needed, modify the user file name and click **Next**.

Result: The **Attribute Set for Policy** window opens. See Figure 7-40.

10 Perform the following steps:

a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.

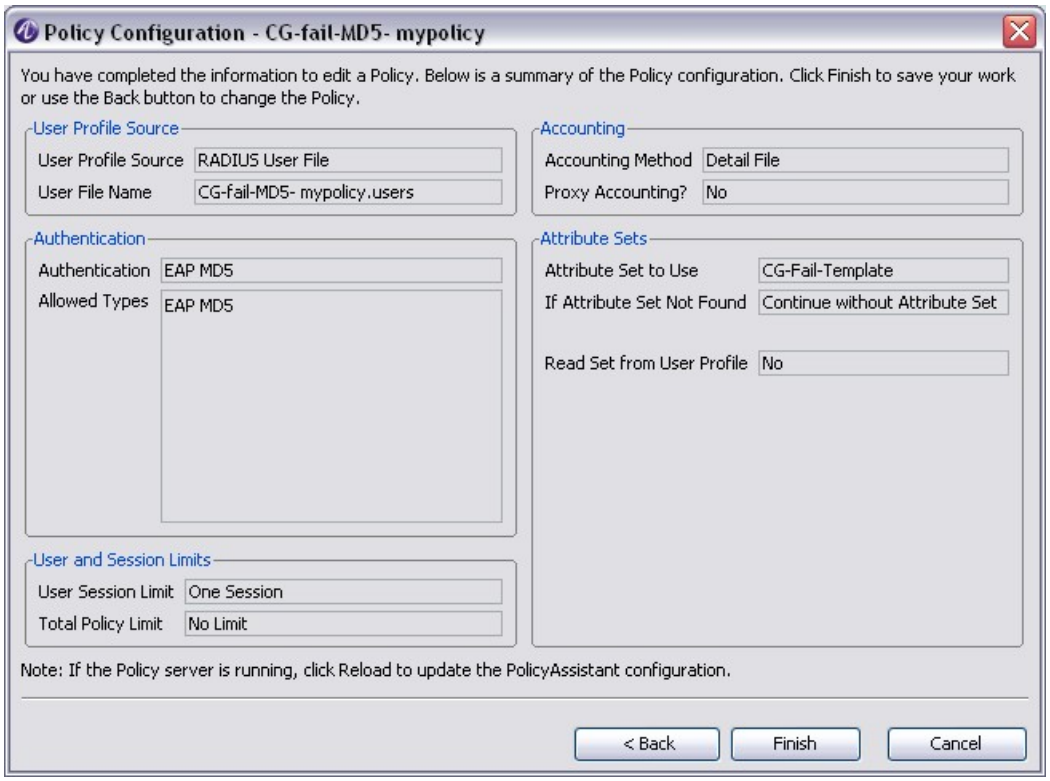
b. From the list of templates, select **CG-Fail-Template**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failure** section, select **Continue without Attribute Set**.

d. Click **Next**.

Result: A window with a summary of policy configuration opens.

Figure 7-42 Policy configuration summary


Policy Configuration - CG-fail-MD5- mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source RADIUS User File
User File Name CG-fail-MD5- mypolicy.users
Accounting
Accounting Method Detail File
Proxy Accounting? No
Authentication
Authentication EAP MD5
Allowed Types EAP MD5
Attribute Sets
Attribute Set to Use CG-Fail-Template
If Attribute Set Not Found Continue without Attribute Set
Read Set from User Profile No
User and Session Limits
User Session Limit One Session
Total Policy Limit No Limit
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

11 Click **Finish** to complete the PolicyAssistant configuration for CG-fail-MD5.

12 Click **Save** to save the policy created.

Configure CG-NoAudit-MD5 authentication with RADIUS User File as user source for CG-NoAudit

Purpose

Use this procedure to configure CG-NoAudit-MD5 authentication with the RADIUS User File as user source and using the PolicyAssistant. This sample policy is for CG-NoAudit status.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens.

2 Click to add a new policy.

Result: The **Policy Configuration** window opens. See Figure 7-6.

3 Enter policy name and click **Next**. For example, enter the policy name as *CG-NoAudit-MD5-mypolicy*.

Result: The **Source for User Profiles** window opens. See Figure 7-7.

4 Select **RADIUS User File** and click **Next**.

Result: The **Authenticating Access Requests** window opens. See Figure 7-8.

5 Expand **EAP Authentication** in the list of **Authentication Types**, select **EAP MD5** and click **Next**.

Result: The **Accounting Configuration** window opens. See Figure 7-9.

6 Select **Save Accounting to a File** and perform the following steps:

a. The file name appears by default. If needed, modify the file name.

b. Select the rollover mode.

c. Click N**ext**.

Result: The **User and Session Limits** window opens. See Figure 7-10.

7 Perform the following steps:

a. In the **User and Session Limits** section, select **One Session**.

b. In the **Policy Limits** section, select **No Limit**.

c. Click **Next**.

Result: The **User File Name Configuration** window opens. See Figure 7-14.

8 The user file name appears by default. If needed, modify the user file name and click **Next.**

Result: The **Attribute Set for Policy** window opens. See Figure 7-40.

9 Perform the following steps:

a. From **Attribute Set to use for this Policy** section, select **Use Attribute Set**.

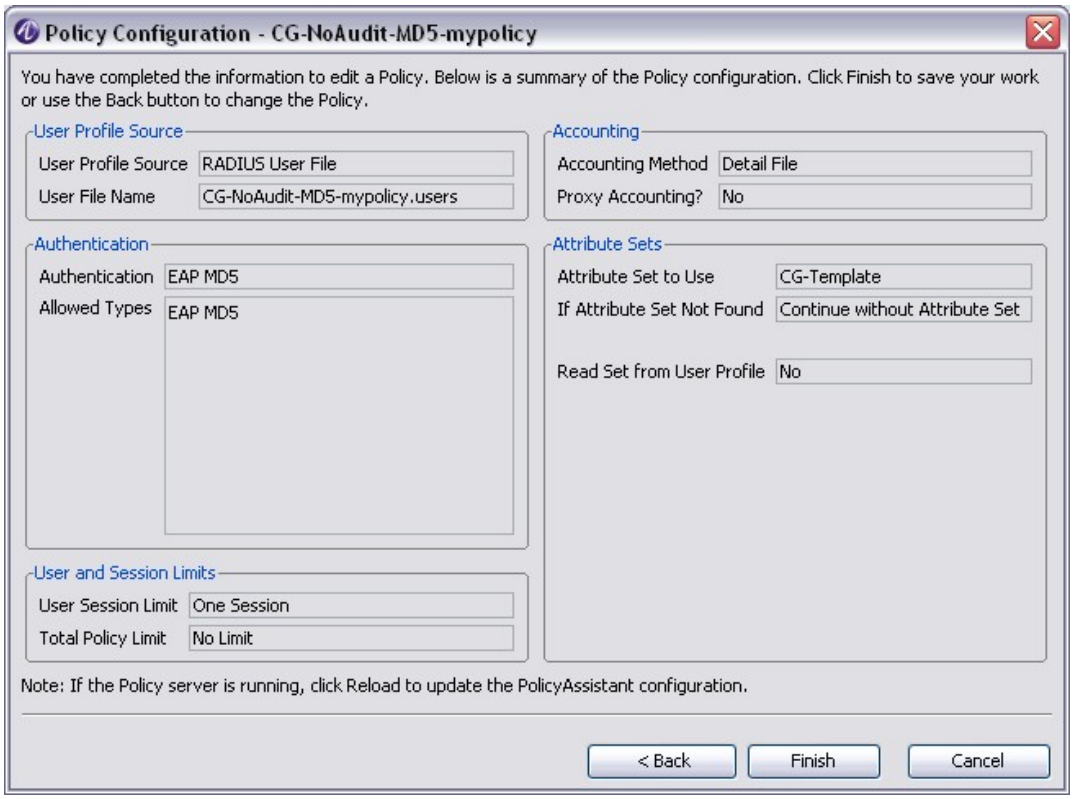
b. From the list of templates, select **CG-Template**. For more information to configure templates, see Configure templates.

c. From the **Attribute Set Lookup Failure** section, select **Continue without Attribute Set**.

d. Click **Next**.

Result: A window with a summary of policy configuration opens. See Figure 7-13.

Figure 7-43 Policy configuration summary


Policy Configuration - CG-NoAudit-MD5-mypolicy
You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.
User Profile Source
User Profile Source RADIUS User File
User File Name CG-NoAudit-MD5-mypolicy.users
Accounting
Accounting Method Detail File
Proxy Accounting? No
Authentication
Authentication EAP MD5
Allowed Types EAP MD5
Attribute Sets
Attribute Set to Use CG-Template
If Attribute Set Not Found Continue without Attribute Set
Read Set from User Profile No
User and Session Limits
User Session Limit One Session
Total Policy Limit No Limit
Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.
< Back
Finish
Cancel

10 Click **Finish** to complete the PolicyAssistant configuration for CG-NoAudit-MD5.

11 Click **Save** to save the policy created.

Configure policy selection rules for CyberGateKeeper

Configure policy selection rule for CyberGateKeeper for Pass Audit

Purpose

Use this procedure to configure CyberGateKeeper-Pass-Audit policy selection rule.

Procedure

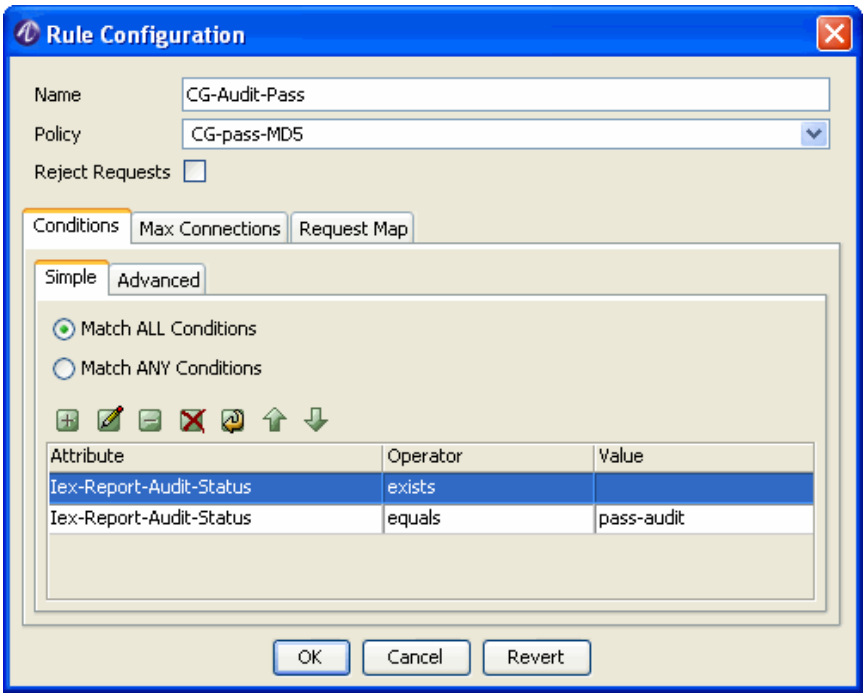
1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens. See Figure 7-1.

2 From the **Policy Selection Rules** tab of the **PolicyAssistant** window, click to add a new rule.

Result: The **Rule Configuration** window opens.

Figure 7-44 Rule Configuration



3 Perform the following steps:

a. Enter the rule name.

b. From the Policy drop-down list, select the policy name. For example, select the Audit Pass policy created for CyberGateKeeper.

c. Click **Conditions** tab.

Result: The **Conditions** panel opens. See Figure 7-2.

4 Click **Simple** tab and perform the following steps:

a. Select **Match ALL Conditions**.

b. Click .

Result: The **Conditions** window opens. See Figure 7-3.

5 Click .

a. Select the attribute **Iex-Report-Audit-Status** and select the operator as **exists**.

b. Select the attribute **Iex-Report-Audit-Status**, select the operator as **equals,** and select the value as **pass-audit**.

c. Click **OK**.

Result: The specified condition displays in the **Simple** panel.

6 Click **OK** to complete.

7 Click **Save** to save the policy selection rule created.

Configure policy selection rule for CyberGateKeeper for Fail Audit

Purpose

Use this procedure to configure CyberGateKeeper-Fail-Audit policy selection rule.

Procedure

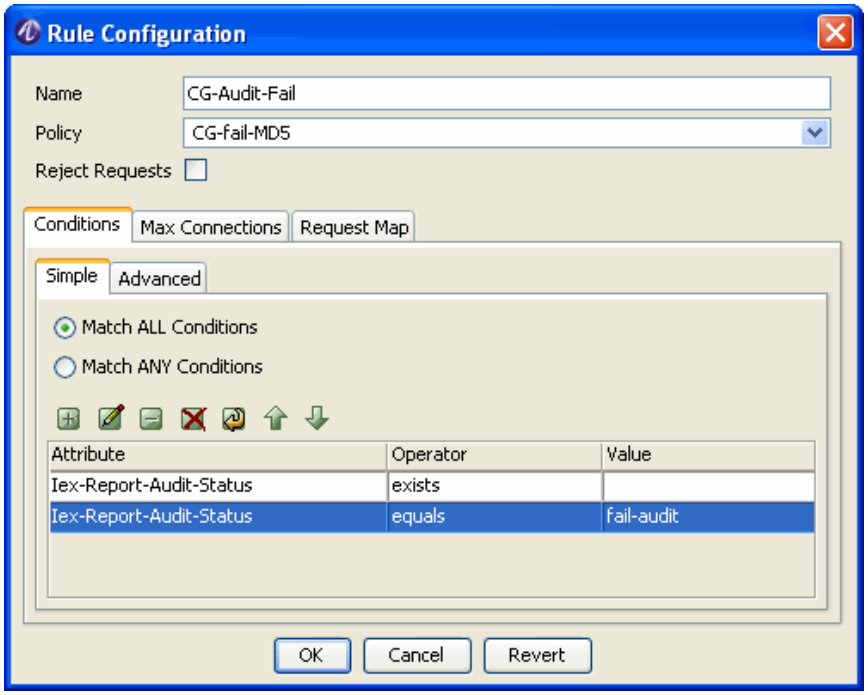
1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens. See Figure 7-1.

2 From the **Policy Selection Rules** tab of the **PolicyAssistant** window, click to add a new rule.

Result: The **Rule Configuration** window opens.

Figure 7-45 Rule Configuration



3 Perform the following steps:

a. Enter the rule name.

b. From the Policy drop-down list, select the policy name. For example, select the Audit Fail policy created for CyberGateKeeper.

c. Click **Conditions** tab.

Result: The **Conditions** panel opens. See Figure 7-2.

4 Click **Simple** tab and perform the following steps:

a. Select **Match ALL Conditions.**

b. Click .

Result: The **Conditions** window opens. See Figure 7-3.

5 Click .

a. Select the attribute **lex-Report-Audit-Status** and select the operator as **exists**.

b. Select the attribute **lex-Report-Audit-Status**, select the operator as **equals,** and select the value as **fail-audit**.

c. Click **OK**.

Result: The specified condition displays on the **Simple** panel.

6 Click **OK** to complete.

7 Click **Save** to save the policy selection rule created.

Configure policy selection rule for CyberGateKeeper for Fail-NoAudit

Purpose

Use this procedure to configure CyberGateKeeper-Fail-NoAudit policy selection rule.

Procedure

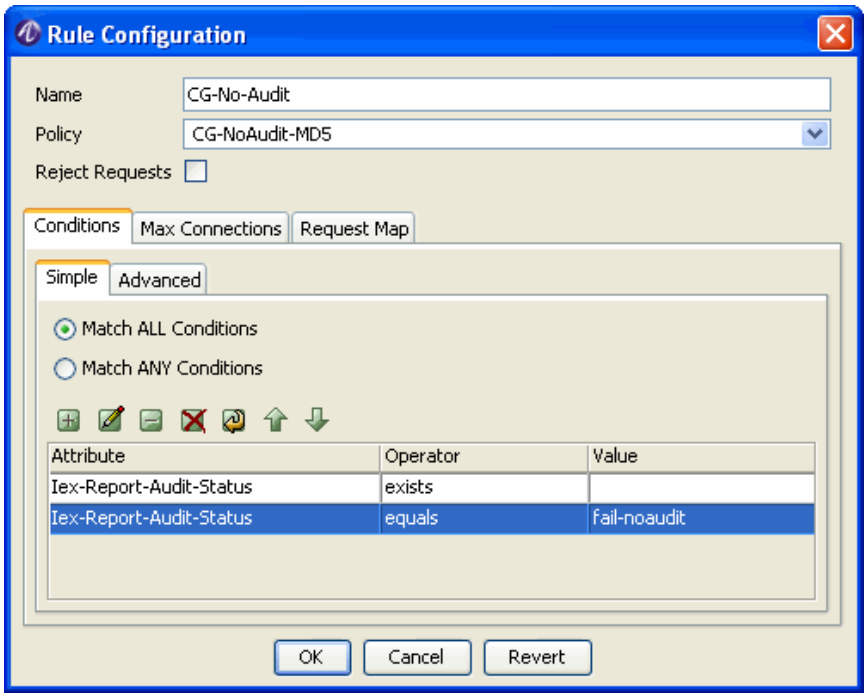
1 From the SMT navigation pane, select **Configuration Tools** -> **PolicyAssistant**.

Result: The **PolicyAssistant** window opens. See Figure 7-1.

2 From the **Policy Selection Rules** of the **PolicyAssistant** window, click to add a new rule.

Result: The **Rule Configuration** window opens.

Figure 7-46 Rule Configuration



3 Perform the following steps:

a. Enter the rule name.

b. From the Policy drop-down list, select the policy name. For example, select the Fail NoAudit policy created for CyberGateKeeper.

c. Click **Conditions** tab.

Result: The **Conditions** panel opens. See Figure 7-2.

4 Click **Simple** tab and perform the following steps:

a. Select **Match ALL Conditions**.

b. Click .

Result: The **Conditions** window opens. See Figure 7-3.

5 Click .

a. Select the attribute **Iex-Report-Audit-Status** and select the operator as **exists**.

b. Select the attribute **Iex-Report-Audit-Status**, select the operator as **equals,** and select the value as **fail-noaudit**.

c. Click **OK**.

Note: For CyberGateKeeper-Default policy select the attribute **Iex-Report-Audit-Status** and the operator **exists**.

Result: The specified condition displays on the **Simple** panel.

6 Click **OK** to complete.

7 Click **Save** to save the policy selection rule created.

8 Configure templates

Overview

Purpose

This chapter describes the procedures to configure the templates.

A template is an attribute group. A template contains all the attributes that are sent by the AAA server to the AAA clients (for example, NAS) after successful authentication. The clients use these attribute values to set up a session. The template defines the service profiles that the 8950 AAA server sends back to NAS clients. For example, the NAS clients are OmniSwitch, OmniAccess, and so on.

In addition, the template defines the set of attribute value pairs, which are verified by the 8950 AAA server before authorizing the client to access the services.

You can create and modify the templates according to the requirements of the enterprise network.

Example 1: User Password can be configured as a *verify* attribute. The 8950 AAA server then verifies the incoming password with the password attribute configured in the verify list.

Example 2: All users connecting through OmniSwitch are assigned a particular VLAN ID. Then, a template can be defined with attribute *filter-id=vlan-id* and apply this template to the policy rule configured in 8950 AAA.

At present, CyberGateKeeper and OmniSwitch templates are available for the user n the enterprise network.

Contents

This chapter covers the following topics.

Create a template	102
Edit a template	107
Delete a template	108

Create a template

Purpose

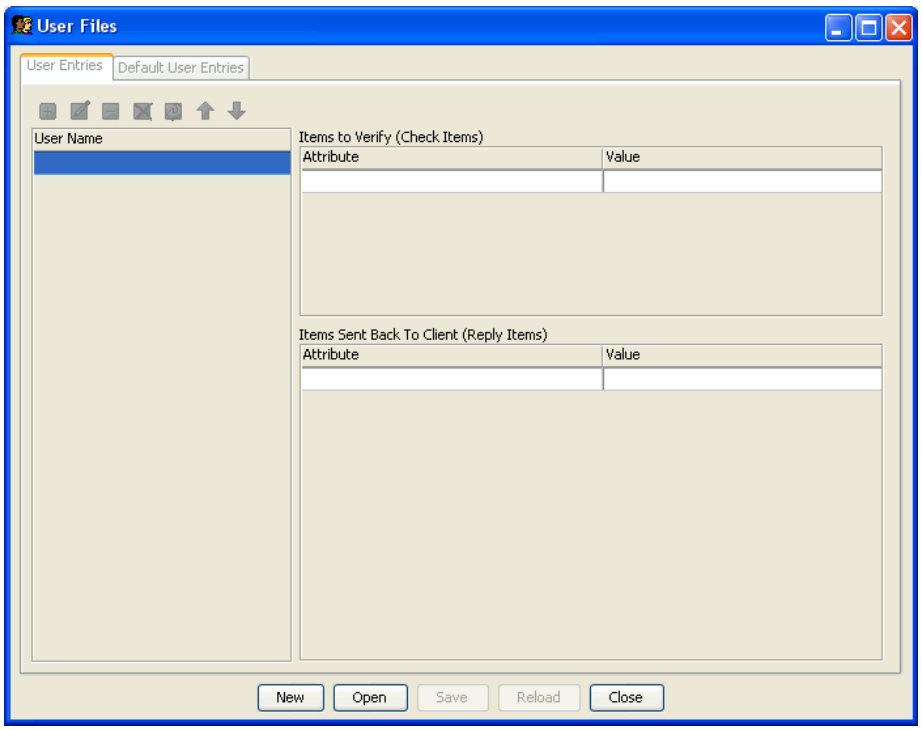
Use this procedure to create a template.

Procedure

1 From the SMT navigation pane, select **File Tools** -> **User Files**.

Result: The **User Files** window opens.

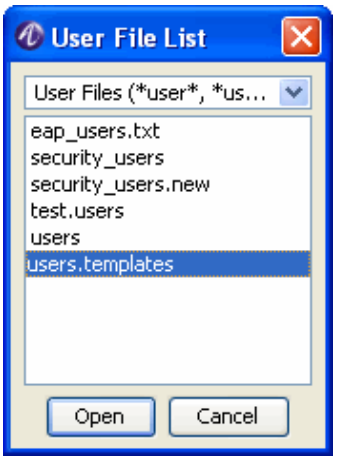
Figure 8-1 User Files



2 Click **Open**.

Result: The **User File List** window opens.

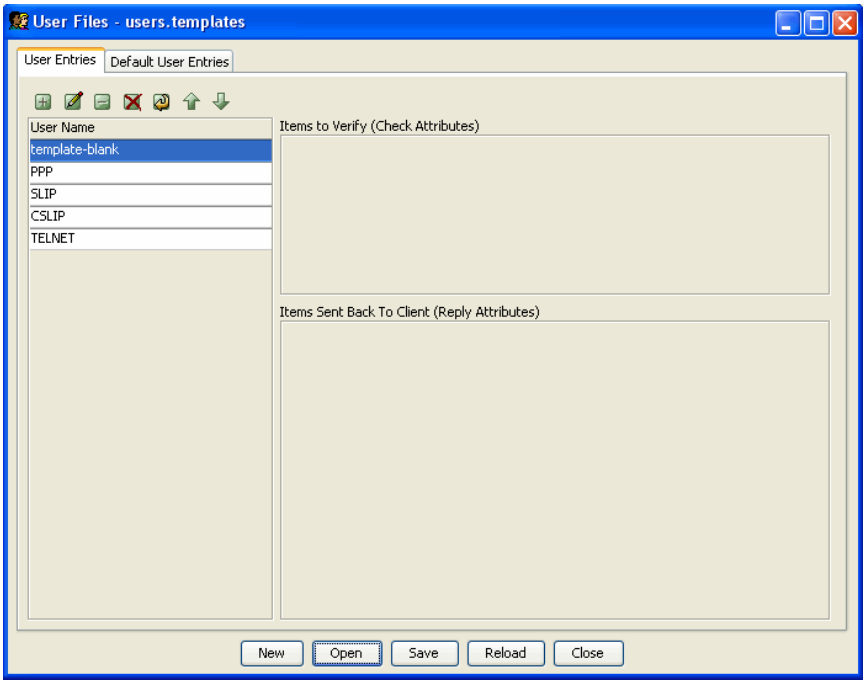
Figure 8-2 User File List



3 Select **users.templates** and click **Open**.

Result: The **User Files- users.templates** window opens.

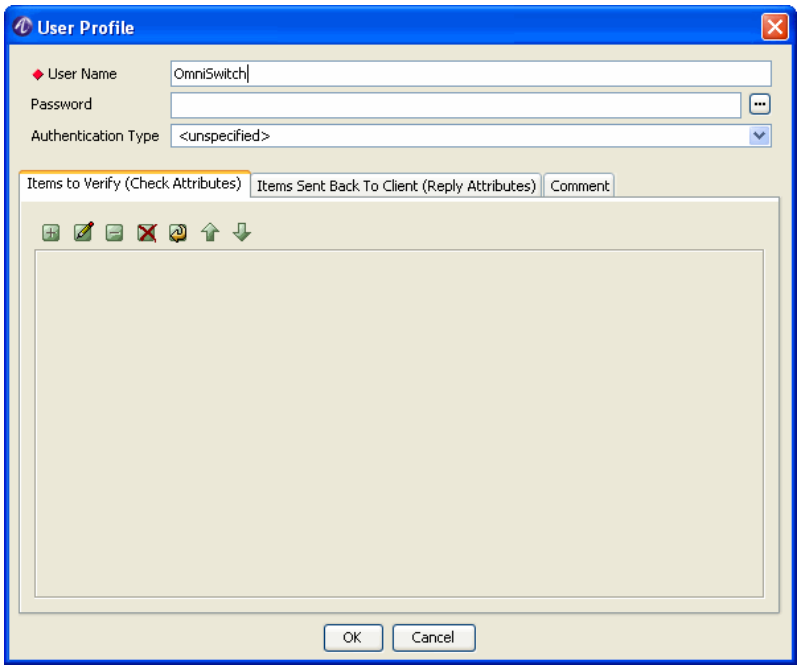
Figure 8-3 User Files-users.templates



4 Click to add a new template.

Result: The **User Profile** window opens.

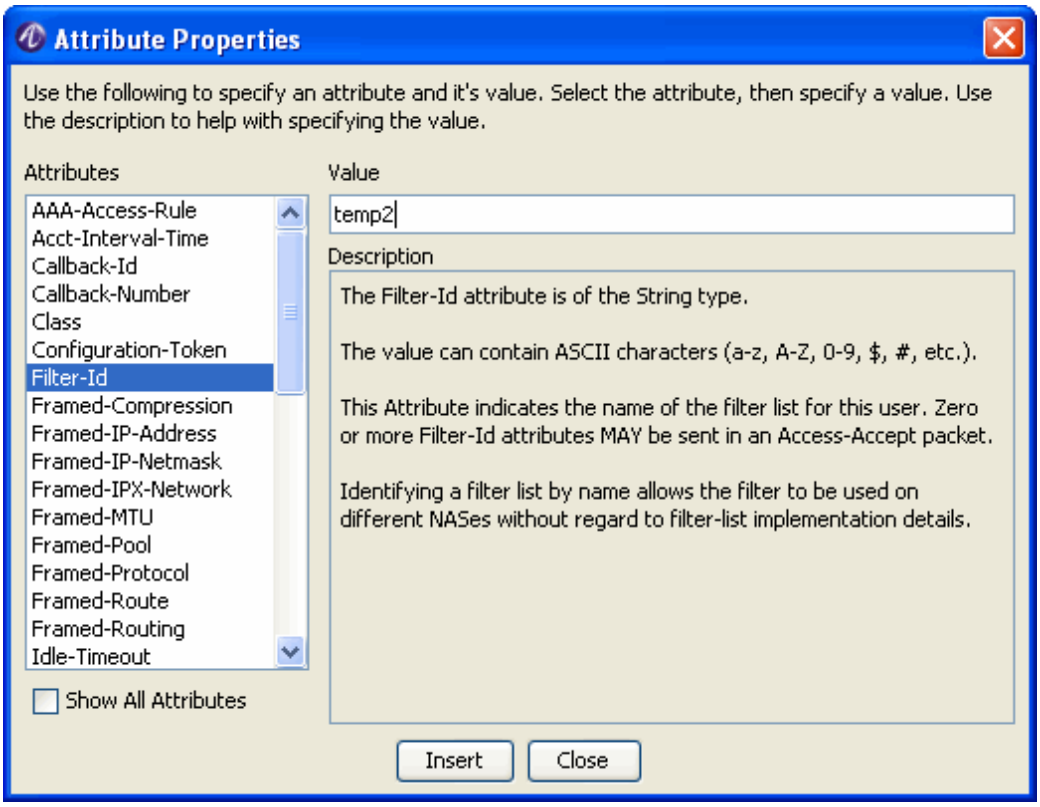
Figure 8-4 User Profile



5 Click **Items Sent Back to Client (Reply Attributes)** tab to add the reply attributes and click .

Result: The **Attribute Properties** window opens.

Figure 8-5 Attribute Properties


Attribute Properties
Use the following to specify an attribute and it's value. Select the attribute, then specify a value. Use the description to help with specifying the value.
Attributes
AAA-Access-Rule
Acct-Interval-Time
Callback-Id
Callback-Number
Class
Configuration-Token
Filter-Id
Framed-Compression
Framed-IP-Address
Framed-IP-Netmask
Framed-IPX-Network
Framed-MTU
Framed-Pool
Framed-Protocol
Framed-Route
Framed-Routing
Idle-Timeout
Show All Attributes
Value
temp2
Description
The Filter-Id attribute is of the String type.
The value can contain ASCII characters (a-z, A-Z, 0-9, $, #, etc.).
This Attribute indicates the name of the filter list for this user. Zero or more Filter-Id attributes MAY be sent in an Access-Accept packet.
Identifying a filter list by name allows the filter to be used on different NASes without regard to filter-list implementation details.
Insert
Close

6 Perform the following steps:

a. Select the required attribute, enter the corresponding value, and click **Insert**.

b. You can insert as many attributes as required.

The **Description** panel displays information on the type of value that can be assigned to an attribute, for example, String type, Enumerated type, IPv4-Address type, and so on.

c. Click **Close** after inserting the attributes.

Result: The **User Profile** window displays the selected attributes.

Note: Figure 8-6 displays a sample OmniSwitch template and Figure 8-7 displays a sample CyberGateKeeper template.

Figure 8-6 User Profile for OmniSwitch

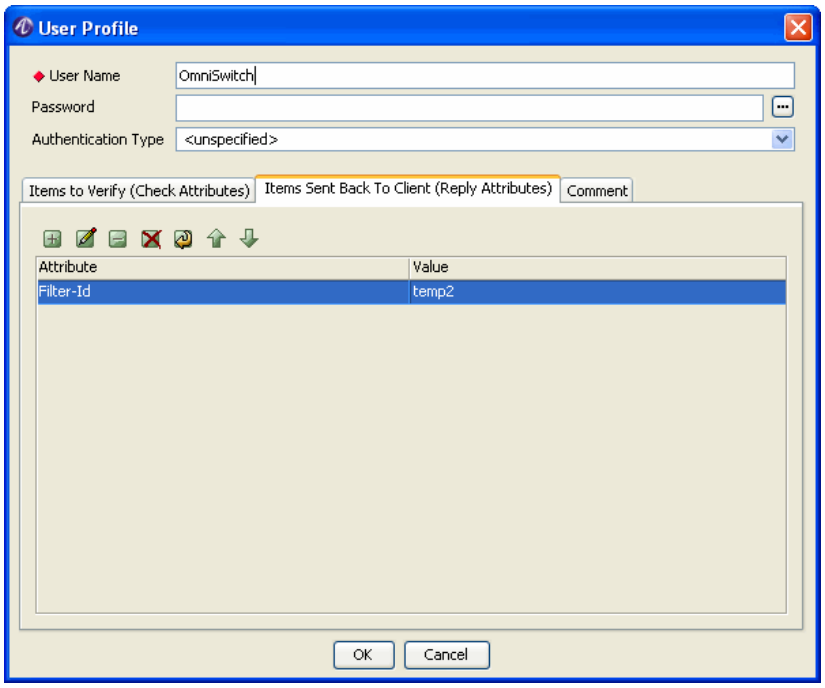
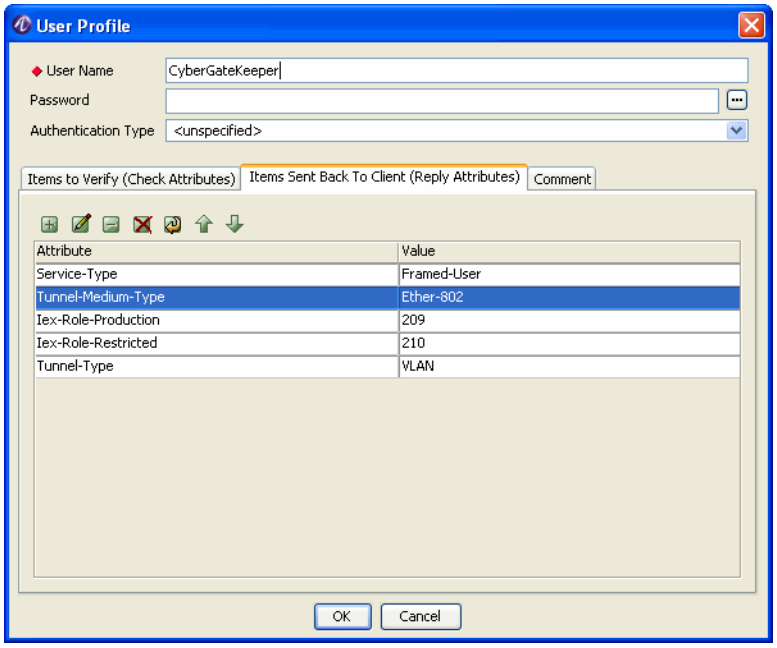


Figure 8-7 User Profile for CyberGateKeeper



7 Click **OK**.

Result: The **User File** window displays the values.

8 Click **Save** to save the template.

Edit a template

Purpose

Use this procedure to edit a template.

Procedure

1 From the SMT navigation pane, select **File Tools** -> **User Files**.

Result: The **User Files** window opens. See Figure 8-1.

2 Click **Open.**

Result: The **User File List** window opens. See Figure 8-2.

3 Select **users.templates** and click **Open**.

Result: The **User Files- users.templates** window opens. See Figure 8-3.

4 Select the required template and click .

Result: The **User Profile** window opens. See Figure 8-4.

5 Click **Items Sent Back to Client** tab.

a. To delete a reply attribute, highlight the attribute and click .

b. To add more reply attributes, click .

c. To modify a reply attribute, highlight the attribute and click .

Result: The **Attribute Properties** window opens. See Figure 8-6.

6 Perform the following steps:

a. Select the required attribute and enter the corresponding value.

b. Click **Insert**.

Result: The **User Profile** window displays the selected attributes.

7 Click **OK.**

Result: The values display on the **User File** window.

8 Click **Save** to save the template.

Delete a template

Purpose

Use this procedure to delete a template.

Procedure

1. From the SMT navigation pane, select **File Tools** -> **User Files**.

   Result: The **User Files** window opens. See Figure 8-1.

2. Click **Open.**

   Result: The **User File List** window opens. See Figure 8-2.

3. Select **users.templates** and click **Open**.

   Result: The **User Files- users.templates** window opens. See Figure 8-3.

4. Select the required template and click to delete the template.
5. Click **Save** to save the template.

Part IV: 8950 AAA configuration

Overview

Purpose

The SMT application provides various tools to configure the 8950 AAA server. This part provides a description of few configuration tools and procedures used in the 8950 AAA server in the enterprise network. For more details, see http://www.8950aaa.com/doc/6.3/SMT.pdf

Contents

This part covers the following chapters.

RADIUS client configuration	111
Vendor-specific attributes	117
8950 AAA policy server	123
8950 AAA Configuration server	139
Derby database	143

9 RADIUS client configuration

Overview

Purpose

This chapter describes the procedures to configure RADIUS clients. RADIUS clients are network access servers, such as wireless access points, 802.1X-capable switches, virtual private network (VPN) servers, and dial-up servers, as they use the RADIUS protocol to communicate with RADIUS servers. For example, in the enterprise network, OmniSwitch, OmniAccess, CyberGateKeeper, and Brick firewall are the RADIUS clients.

When you configure a RADIUS client in the enterprise network, you designate the following properties:

- Client name
- IP address
- Client-Vendor
- Shared secret
- Message Authenticator attribute, and so on.

These properties allow the clients to set up a secure network connection with the 8950 AAA server.

Contents

This chapter covers the following topics.

Any RADIUS client configuration	112
Identifying a client type	115

Any RADIUS client configuration

Purpose

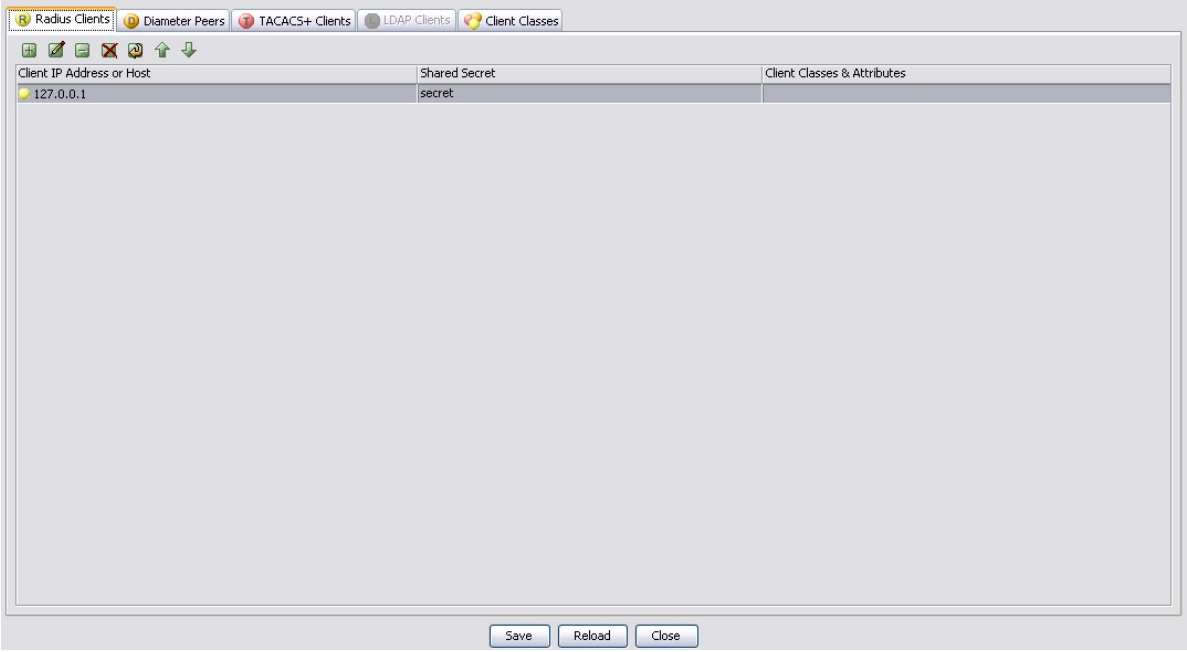
Use this procedure to configure RADIUS clients.

Procedure

1 From the SMT navigation pane, select **Configuration Tools** -> **Client / Peers**.

Result: The **Client Properties** window opens.

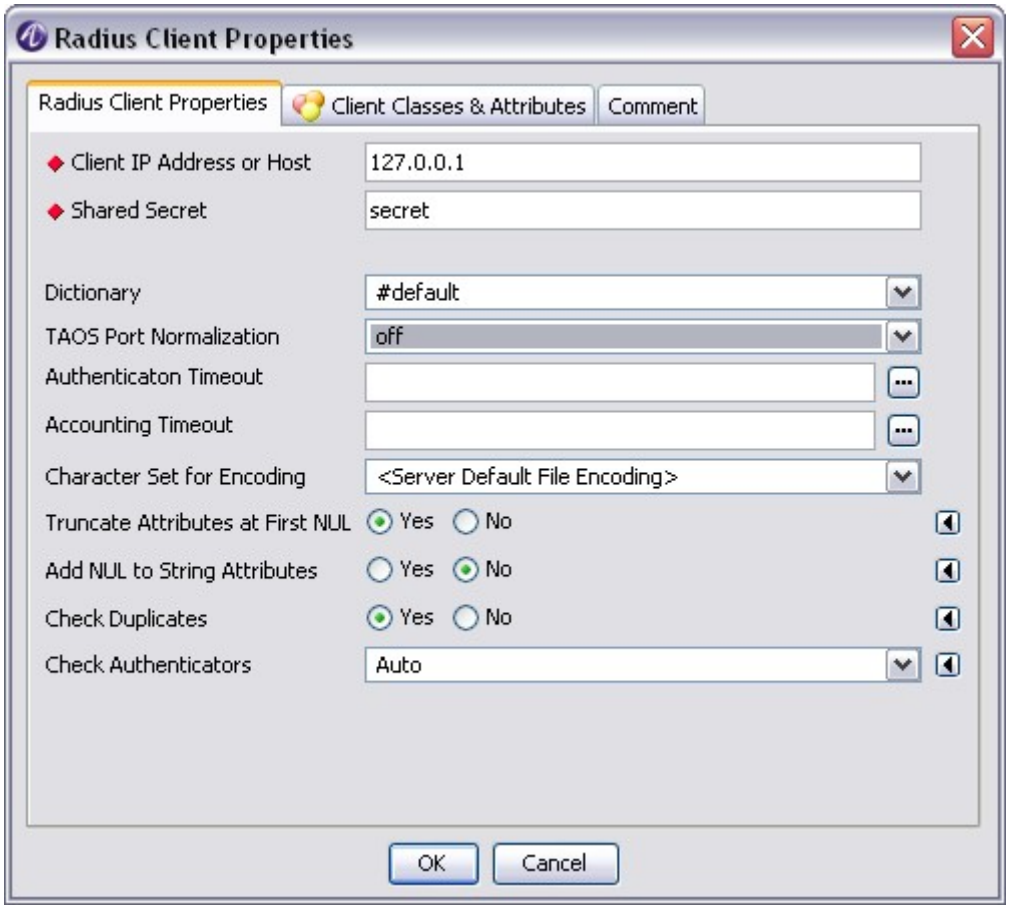
Figure 9-1 Client Properties



2 Click to add a new RADIUS client.

Result: The **Radius Client Properties** window opens.

Figure 9-2 Radius Client Properties



3 Use Table 9-1 to enter the information and click **OK**.

Table 9-1 RADIUS client Properties

Field	Description	Type	Value
Client IP Address or Host	Enter the Domain name, IP Address, range of IP addresses, or a CIDR block of addresses.	Text	Default value: No
Shared Secret	Shared secret between AAA and client.	Text	Default value: No
Dictionary	Enter the name of the dictionary to use for the client class definition. For an enterprise network, select default codec.	Dictionary codec	Default value: No
TAOS Port Normalization	Select the version of TOAS to get the real NAS port number out of the NAS port info. Use this field if your NASs are running TAOS.	Dictionary Attribute List	Default value: No

Field	Description	Type	Value
Authentication Timeout	Enter time, in milliseconds. The Policy server waits for this time before it discards authentication requests. This field overrides the Client Timeout value for authentications only.	Duration with default time unit of milliseconds	Default value: No
Accounting Timeout	Enter time, in milliseconds. The Policy server waits for this time before it discards accounting requests. This field overrides the Client Timeout value for accounting requests only.	Duration with default time unit of milliseconds	Default value: No
Character Set for Encoding	Select from the drop-down list the character set that is used to encode string attributes in requests. For an enterprise network, select default character set.	Character set	Default value: No
Truncate Attributes at First NUL	This field specifies if the NAS devices send NUL characters in their attributes. If enabled, attributes are truncated at the first NUL found in the value. If disabled, the attribute values are not truncated.	Boolean	Default value: Yes
Add NUL to String Attributes	This field specifies if the NAS devices send NUL characters in their attributes. If enabled, a NUL is appended to the end of plain string attributes in response requests to the NAS.	Boolean	Default value: No
Check Duplicates	Duplicates are detected by a combination of the Source IP, Source Port, and Packet Authenticator. If enabled, the server checks to see if the request received is a duplicate of a previously received request. This property can be set on a pre-client basis in the Client Properties.	Boolean	Default value: Yes
Check Authenticators	The drop-down list box displays the Auto, On, or OFF options. If enabled, the Policy server checks the request authenticator and if not verified, the request is dropped.	List of values	Default value: Auto

Note:

You can also configure the RADIUS client in the following two ways:

– By specifying a **range of IP addresses** in the **Client IP Address or Host** field: This type of configuration sets aside a block of unique IP addresses to be used for the client or host applications.

– By specifying a **CIDR block of IP addresses**: Here, the IP address is followed by a slash and the number (in decimal) of bits used for the network part, also called the *routing prefix*. For example, an IPv4 address and its subnet mask are 192.0.2.1 and 255.255.255.0, respectively. The CIDR notation for the same IP address and subnet is 192.0.2.1/24, because the first 24 bits of the IP address indicate the network and subnet. CIDR provides the possibility of fine-grained routing prefix aggregation, also known as *supernetting* or *route summarization*.

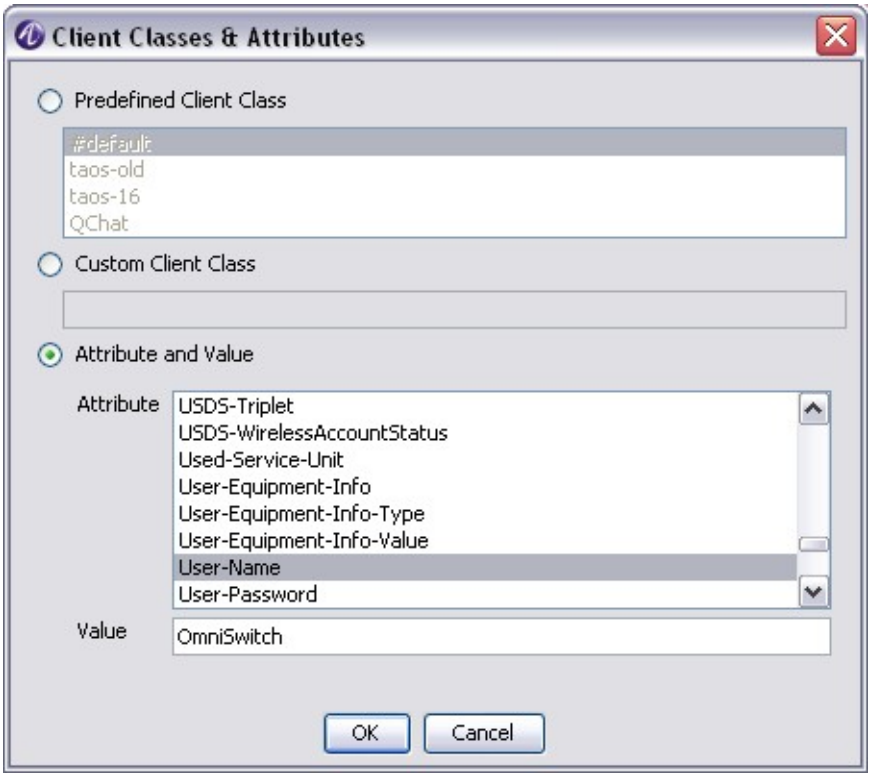
Identifying a client type

This feature allows you to distinguish each RADIUS client. You can assign a common attribute to a group of RADIUS clients belonging to one single category. For example, you can categorize all OmniSwitch client devices by assigning a common attribute, **User-Name** as ***OmniSwitch***. Assigning attributes helps in configuring all clients belonging to one category as a single entity.

The **Insert Row Wizard** action button in this tab allows you to select the required type of client and to select the configuration options for that type of client. The **Insert a record** action button allows you to set the client classes and attributes from the following list of options:

- Select from a **Predefined Client Class**
- Add a **Custom Client Class**
- Select or add the attribute and the value from the list

Figure 9-3 Client Classes and Attributes



10 Vendor-specific attributes

Overview

Purpose

This chapter describes the procedures to add the vendor and vendor-specific attributes to the dictionary. This feature allows the 8950 AAA to support any type of 802.1x access points in an enterprise network. The 8950 AAA provides the ability to specify RADIUS attributes that are returned with a RADIUS response message. These RADIUS attributes can be specified for each remote access policy and are configurable. Some NAS vendors use vendor-specific attributes (VSAs) to provide functionality that is not supported in standard attributes. 8950 AAA enables you to create or edit VSAs to take advantage of proprietary functionality supported by some NAS vendors.

Example: To integrate CyberGateKeeper with 8950 AAA server in the enterprise network, the attribute ***Iex-Report-Audit-Status***, a vendor-specific attribute, is added to the dictionary.

Contents

This chapter covers the following topics.

Add vendor to the dictionary	118
Add vendor-specific attributes to the dictionary	119

Add vendor to the dictionary

Purpose

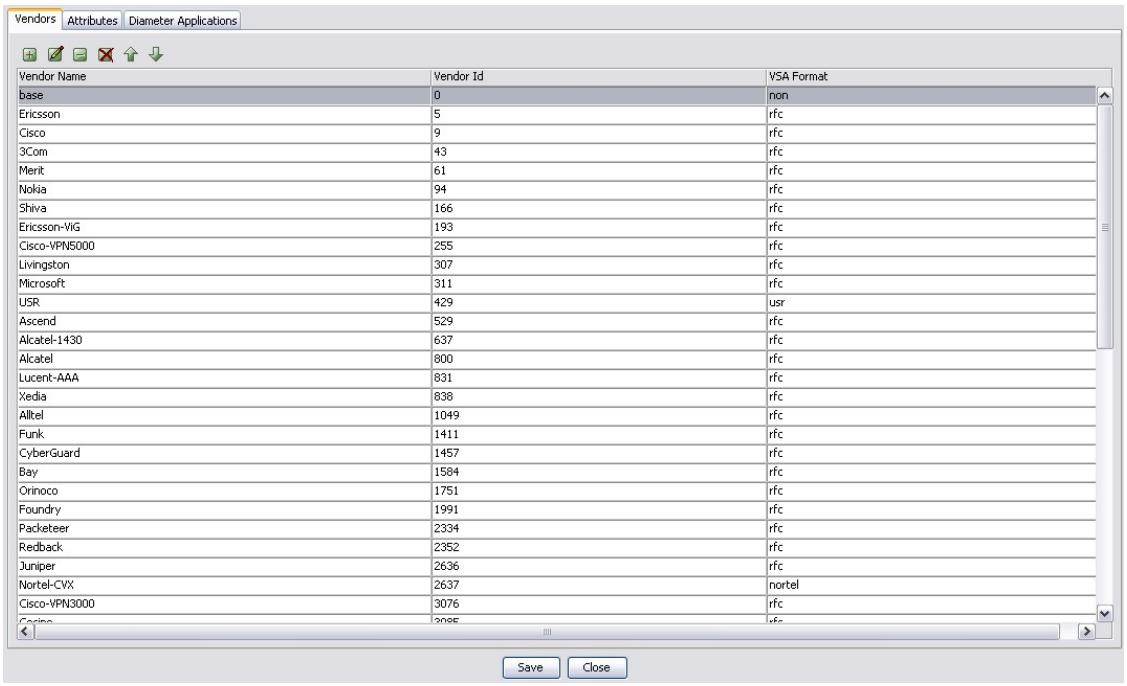
Use this procedure to add vendor to the dictionary.

Procedure

1 From the SMT navigation pane, select **File Tools** -> **Dictionary Editor**.

Result: The **Vendors** window opens.

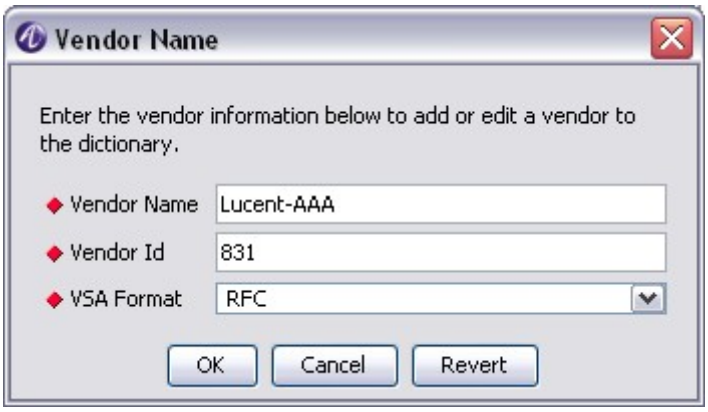
Figure 10-1 Vendors



2 Click .

Result: The **Vendor Name** window opens.

Figure 10-2 Vendor Name



3 Enter the following in the fields in the window displayed:

- **Vendor Name** – Enter the name of the vendor as specified.
- **Vendor ID** – Enter the unique vendor number. The Internet Assigned Numbers Authority (IANA) assigns these numbers to each registered vendor.
- **VSA Format** – From the drop-down box, select a VSA format.

4 Click **OK**.

Result: The vendor information is added to the dictionary and the table is updated.

Add vendor-specific attributes to the dictionary

The **Attributes** tab allows you to configure and manage the attributes related to a vendor in the 8950 AAA.

Purpose

Use this procedure to configure the vendor-specific attributes.

Procedure

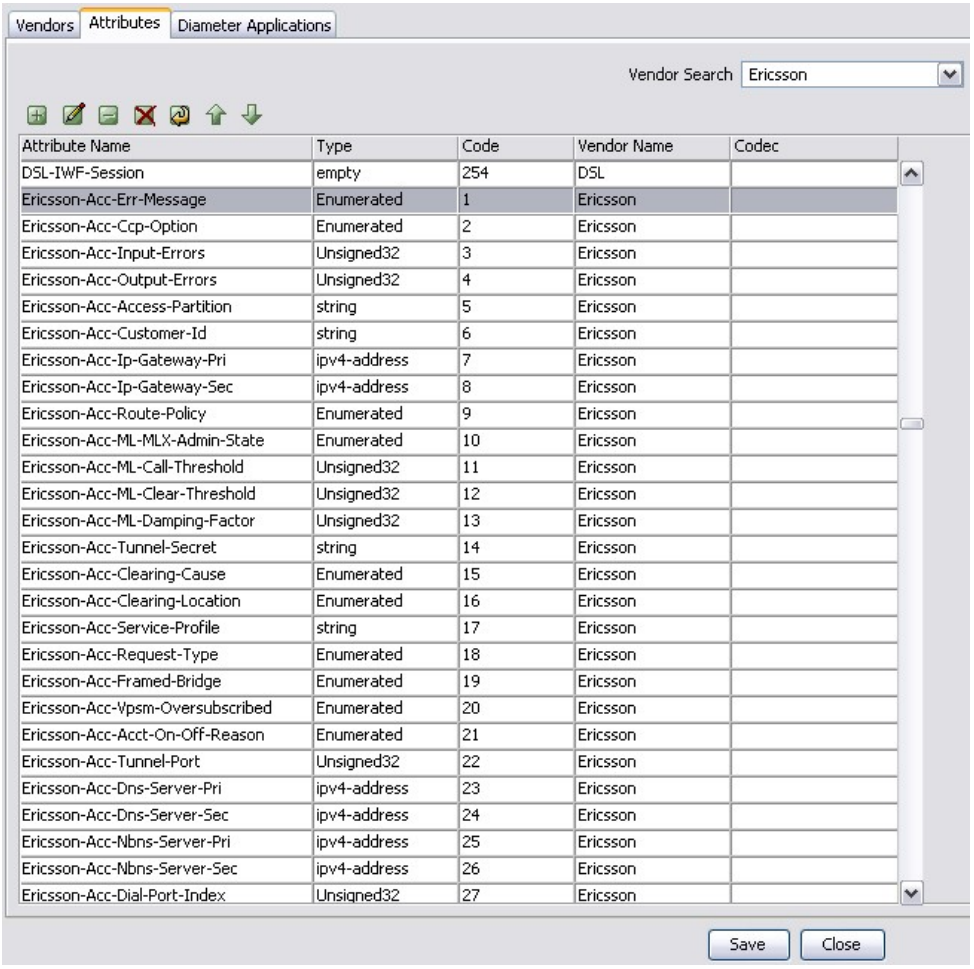
1 From the SMT navigation pane, select **File Tools** -> **Dictionary Editor**.

Result: The **Vendors** window opens. See Figure 10-1.

2 Select **Attributes** tab.

Result: The **Attributes** window opens.

Figure 10-3 Vendors - Attributes

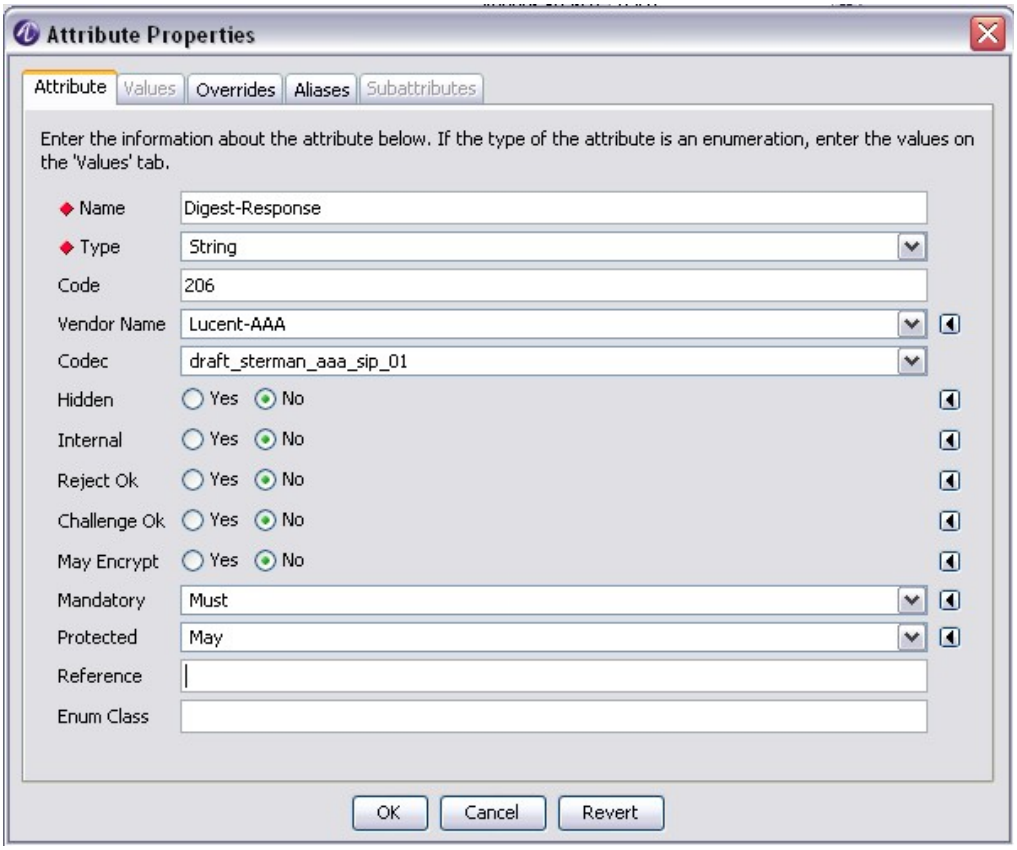


Note: To display the attributes based on the name of the vendor, select the name of the vendor in the drop-down box in the **Vendor Search** field.

3 To add attributes to the dictionary, click .

Result: The **Attributes Properties** window opens.

Figure 10-4 Vendors - Attributes Properties



4 Use Table 10-1 to enter the information and click **OK**.

Table 10-1 Vendor attributes

Field	Description	Type	Value
Name	Name of the vendor-specific attribute to be added.	Text	Default value: No
Type	Type of the attribute, such as String, IP Address, Integer, and so on.	Dictionary type list	Default value: No
Code	The attribute code.	Signed integer	Default value: No
Vendor Name	Name of the vendor.	List of values	Default value: Base
Codec	The code encoder and decoder	List of values	Default value: No

Field	Description	Type	Value
Hidden	If set to true, the value of this attribute is not displayed in the server and accounting logs.	Boolean	Default value: No
Internal	If set to true, this attribute is marked as an internal attribute and is used only in 8950 AAA.	Boolean	Default value: No
Reject Ok	Unless set to true, this attribute is not included in RADIUS access-reject.	Boolean	Default value: No
Challenge Ok	Unless set to true, this attribute is not included in RADIUS access-challenge.	Boolean	Default value: No
May Encrypt	If enabled, indicates that the value for this attribute is encrypted.	Boolean	Default value: No
Mandatory	Records M-Bit rule for diameter.	List of values	Default value: Must
Reference	Reference document for this attribute. For example, RFC number.	Text	Default value: No
Enum Class	Declares a managed enumeration.	Text	Default value: No

Related Information

Values tab: The Values tab allows you to add the enumeration values for the attributes. The codes entered here are unique to the values for this attribute. Enter the Aliases as provided by the vendors. Ensure to separate the Aliases with a comma.

Overrides tab: The Overrides tab allows you to enter codec overrides for this attribute.

Aliases tab: The Aliases tab allows you to enter the different attribute names for the same functionality.

11 8950 AAA policy server

Overview

Purpose

This chapter provides a description of the policy server and various configuration procedures for the policy server used in the 8950 AAA server. The enterprise user can use the Policy server, which uses the PolicyFlow language, to configure complex policy rules, which cannot be done using the PolicyAssistant.

Contents

This chapter covers the following topics.

8950 AAA policy server	123
Start policy server	124
Configure delimiters for policy server	134
Configure timeout properties of policy server	136

8950 AAA policy server

Policy server handles the authentication, authorization, and accounting requests in the 8950 AAA server. It is a multi-threaded system designed to handle multiple tasks concurrently.

The 8950 AAA offers a built-in programming language for writing custom AAA policy applications. The PolicyFlow™ language allows the system to conform to any possible policy scenario. PolicyFlow architecture built on Java programming language is flexible and extensible.

Policy server is an execution engine for PolicyFlow. During operation, policy server collects various system variables and generates alerts based on pre-configured threshold

values. It supports Telnet and SSH-based Command Line Interface (CLI) through Admin console. Policy server supports CLI for remote login and debugging purposes. Administrators can use this CLI for executing commands for administrative purposes. Policy server has a built-in web server used for the following purposes:

- Display server information
- Display authentication and accounting statistics
- View documentation
- Access to User Provisioning Tool (UPS)
- View deployed SOAP services

Policy server is a platform for supporting various functions and components of 8950 AAA. The important functions are listed as follows:

- RADIUS listener for handling protocol-specific AAA requests
- Built in session database for managing the user sessions
- SNMP MIB and trap support
- Extensive logging capabilities with multiple log channels
- Hosts embedded Derby database
- Server monitoring and statistics tools

Start policy server

Purpose

You can start the policy server in one of the following ways:

- From the SMT
- From the command line window
- As Windows service application

Before you begin

Ensure to start the SMT before you start the policy server.

From the SMT

Related information

The tool bar of the SMT displays icons to start Policy Server and Configuration Server. The figure shows the position of the Policy Server tool icon.

Procedure

1. From the SMT navigation pane, click the Policy Server tool icon.
2. Select **Start Server** in the drop-down list.

   Result: The policy server starts and the status changes to green.

From the command line window

Procedure

1. In the command line window, navigate to the <*Installed AAA*>*bin* folder.
2. Enter the command **`aaa-start policy`**.

   Result: The policy server starts and the status changes to green.

As Windows service application

Before you begin

Ensure you have the right local windows security enhancements before you begin this procedure. The user should have administrative privileges and needs to be authenticated.

Follow this procedure to configure the security policy on the local system:

1. From the **Start** menu, navigate to **Control Panel** and select **Administrative Tools**.
2. In the **Administrative Tools** window, select **Local Security Settings**.
3. Double-click **Act as part of the operating system**.
4. Click **Add User or Group** and enter the domain name and the user name.
5. Click **OK** to save changes. Accept all warnings.

The local security policy is now configured.

Procedure

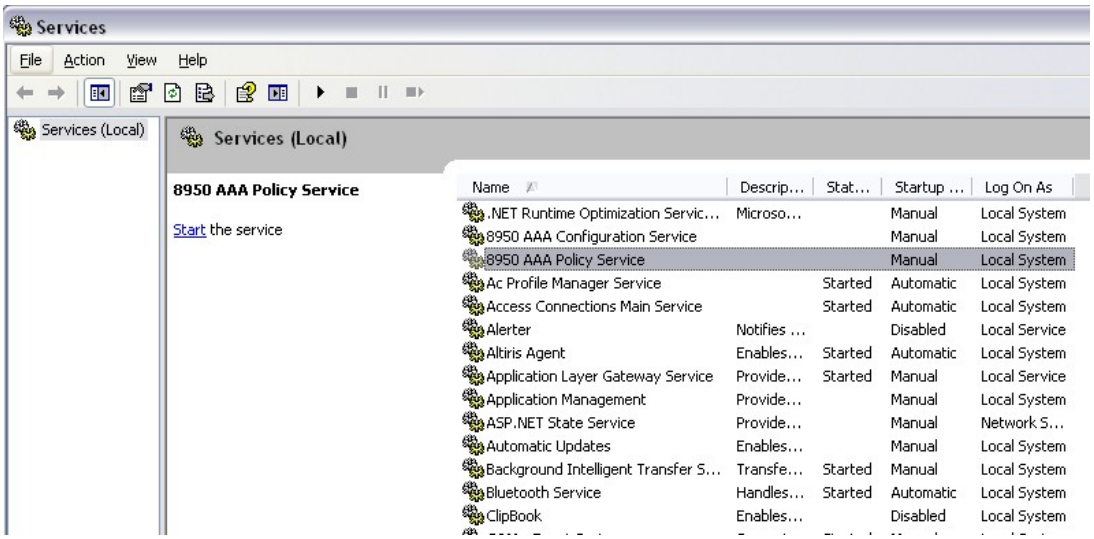
1 Click **Start** button to display the **Start** menu.

2 Navigate to **Control Panel**.

3 Click **Administrative Tools** -> **Services**.

Result: The **Services** window opens.

Figure 11-1 Windows Services

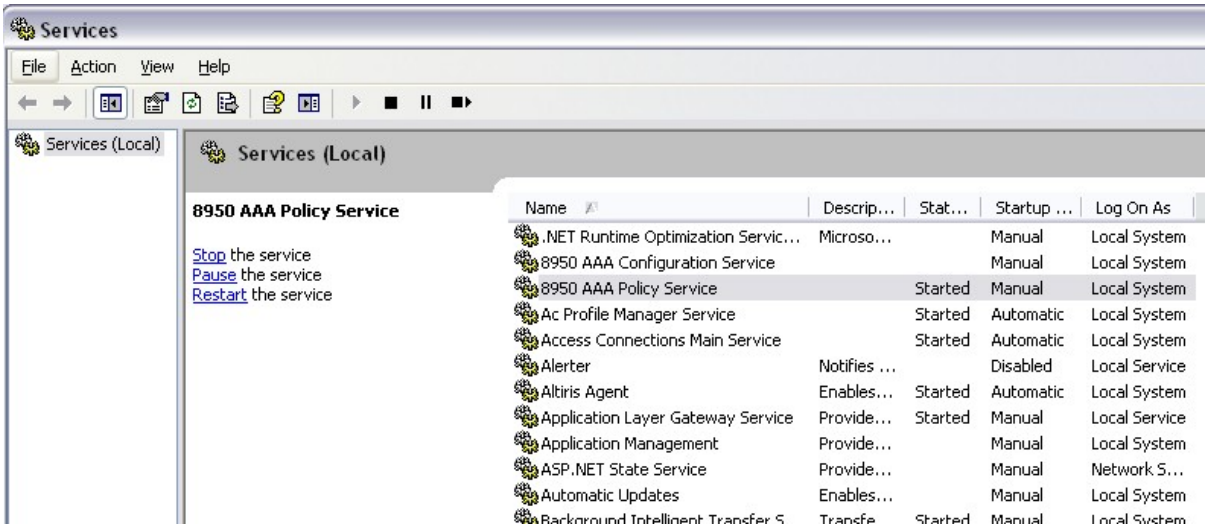

Services
File Action View Help
Services (Local)
Services (Local)
8950 AAA Policy Service
Start the service
Name Descrip... Stat... Startup ... Log On As
.NET Runtime Optimization Servic... Microso... Manual Local System
8950 AAA Configuration Service Manual Local System
8950 AAA Policy Service Manual Local System
Ac Profile Manager Service Started Automatic Local System
Access Connections Main Service Started Automatic Local System
Alerter Notifies ... Disabled Local Service
Altiris Agent Enables... Started Automatic Local System
Application Layer Gateway Service Provide... Started Manual Local Service
Application Management Provide... Manual Local System
ASP.NET State Service Provide... Manual Network S...
Automatic Updates Enables... Manual Local System
Background Intelligent Transfer S... Transfe... Started Manual Local System
Bluetooth Service Handles... Started Automatic Local System
ClipBook Enables... Disabled Local System

4 Select **8950 AAA Policy Service** from the list of applications.

5 In the left-hand panel, click **Start the service**, or right-click and select **Start**.

Result: The policy server starts as a Windows service application. The status changes to **Started**.

Figure 11-2 Windows Services


Services
File Action View Help
Services (Local)
Services (Local)
8950 AAA Policy Service
Stop the service
Pause the service
Restart the service
Name Descrip... Stat... Startup ... Log On As
.NET Runtime Optimization Servic... Microso... Manual Local System
8950 AAA Configuration Service Manual Local System
8950 AAA Policy Service Started Manual Local System
Ac Profile Manager Service Started Automatic Local System
Access Connections Main Service Started Automatic Local System
Alerter Notifies ... Disabled Local Service
Altiris Agent Enables... Started Automatic Local System
Application Layer Gateway Service Provide... Started Manual Local Service
Application Management Provide... Manual Local System
ASP.NET State Service Provide... Manual Network S...
Automatic Updates Enables... Manual Local System

To close the service application, click **Stop the service** in the left-hand panel, or right-click and select **Stop**.

Configure 8950 AAA protocol properties for policy server

Overview

RADIUS properties specify the configuration values for policy server, when processing RADIUS requests.

Attributes properties specify how policy server handles RADIUS attributes.

RADIUS Request Properties specify how policy server handles RADIUS requests.

Purpose

Use this procedure to configure the properties of policy server for processing RADIUS requests.

Procedure

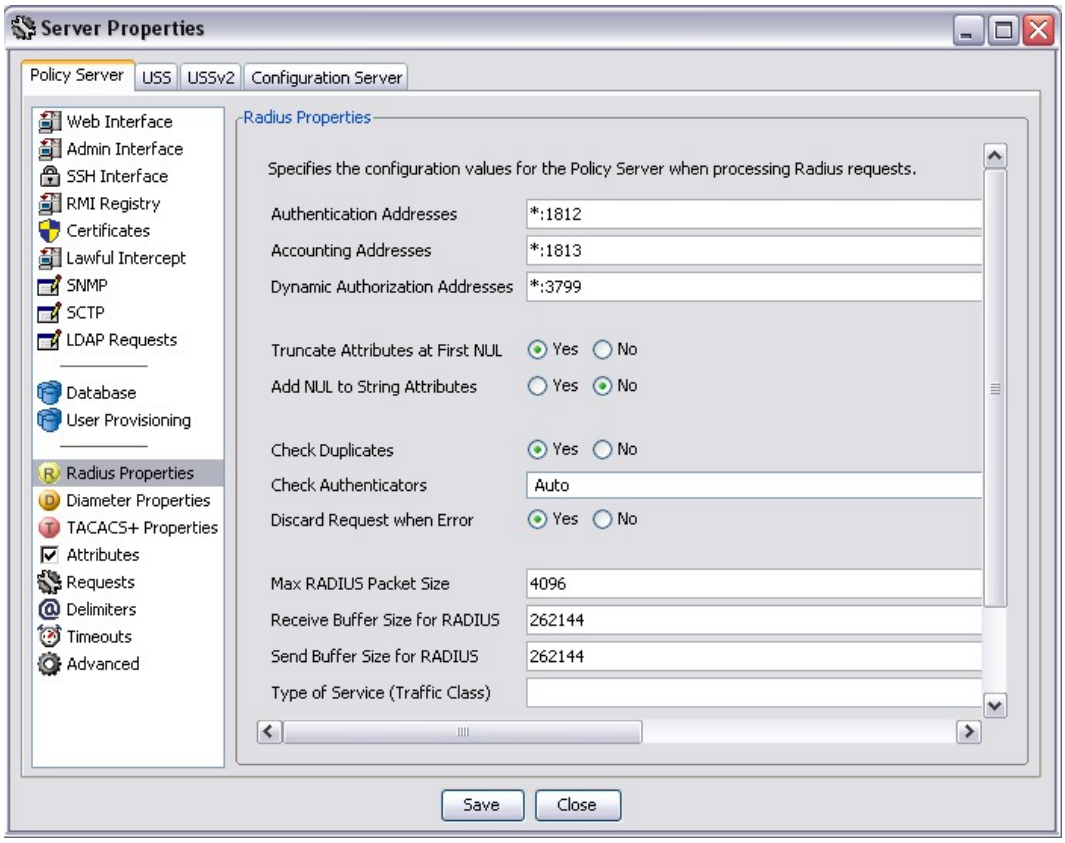
1 From SMT navigation pane, select **Configuration Tools** -> **Server Properties**.

Result: The **Server Properties** window opens.

2 Select **Policy Server->Radius Properties**.

Result: The **Radius Properties** panel opens.

Figure 11-3 Radius Properties



3 Use Table 11-1 to enter the required information.

Table 11-1 RADIUS Properties

Field	Description	Type	Value
Authentication Addresses	Enter the listening addresses for authentication requests. This field is a comma-separated list of address:port values. **Note:** If this property is set to zero (0), policy server does not process the RADIUS authentication requests.	Network address format: *xxx.xxx.xxx.xxx:<port>*	Default value: *:1645 or *:1812
Accounting Addresses	Enter the listening addresses for accounting requests. This field is a comma-separated list of address:port values. **Note:** If this property is set to zero (0), policy server does not process the RADIUS accounting requests.	Network address format: *xxx.xxx.xxx.xxx:<port>*	Default value: *:1646 or *:1813

Field	Description	Type	Value
Dynamic Authentication Addresses	Enter the listening address for dynamic authentication requests. This field is a comma-separated list of address:port values. If the address is omitted, default address *. is considered and port omitted default of 3799 is considered.	Network address format: *xxx.xxx.xxx.xxx:<port>*	Default value: *:3799
Truncate Attributes at First NUL	If enabled, attributes are truncated at the first NUL found in the value. If disabled, the attribute values are not truncated. Enables support for NAS devices that send NUL characters in their attributes.	Boolean	Yes No
Add NUL to string attributes	If enabled, a NUL is appended to the end of plain string attributes in response requests to the NAS. This property enables support for NAS devices that send NUL characters in their attributes.	Boolean	Yes No
Check Duplicates	If enabled, the server checks to see if the request received is a duplicate of a previously received request. Duplicates are detected by a combination of the Source IP, Source Port, and Packet Authenticator. The default setting is true. This property can be set on a per-client basis in the Client properties.	Boolean	Yes No
Check Authenticators	If enabled, the policy server checks the request authenticator and if not verified, the request is dropped.	One of the list values	Off Auto On
Discard request when error	If enabled, the policy server discards packets when a method returns an error.	Boolean	Yes No

Field	Description	Type	Value
	If not enabled, the policy server rejects the packet.		
Max RADIUS packet size	Enter the maximum RADIUS packet size that is allowed.	Whole number	Default value: 4096 Bytes
Receive buffer size for RADIUS	Enter the size of the system UDP receive buffer assigned to the local socket.	Whole number	Default value: 262144
Send buffer size for RADIUS	Enter the size of the system UDP send buffer assigned to the local socket.	Whole number	Default value: 262144
Type of Service (Traffic Class)	Enter the traffic class or type-of-service octet in the RADIUS IP header.	Whole number	Range: 0-255
Response Cache Timeout Enabled	If enabled, the policy server caches responses for the time specified in the corresponding timeout property. If not enabled, responses are not cached.	Boolean	Yes No
Response Cache Timeout	Specify the response cache timeout. When responding to the RADIUS requests, the policy server remembers (cache) the responses. If the response is sent, but lost and the NAS resends the same request, the policy server responds with the cached response. Policy server does process the request again. This property sets the time for which the policy server keeps cached entries before discarding them.	Use , to specify the duration.	Default value: 60 s

Result: The configured values are displayed on the **Radius Properties** panel.

4 Use Table 11-2 to enter the information.

Table 11-2 TACACS+ Properties

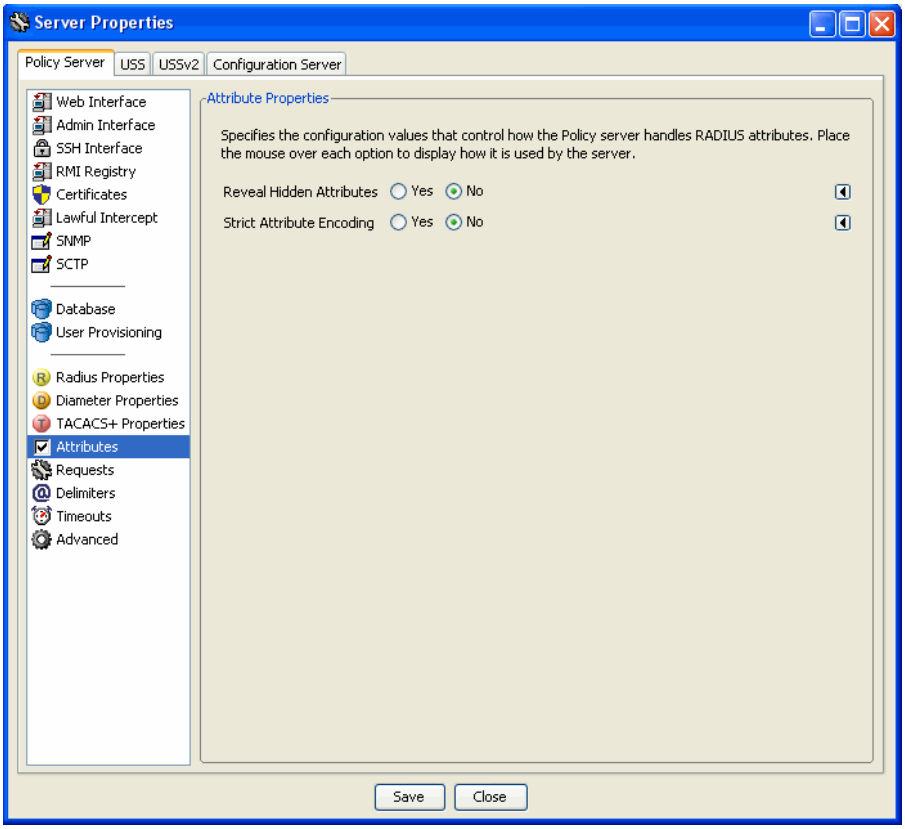
Field	Description	Type	Value
TACACS+ Address	Enter the listener address that the policy server uses for the TACACS+ service.	Network address format: *xxx.xxx.xxx.xxx:<port>*	Default value: *:49

Result: The configured values are displayed on the **Terminal Access Controller Access-Control System Plus Properties** panel.

5 Select **Attributes**.

Result: The **Attributes Properties** panel opens.

Figure 11-4 Attributes Properties



6 Use Table 11-3 to enter the information.

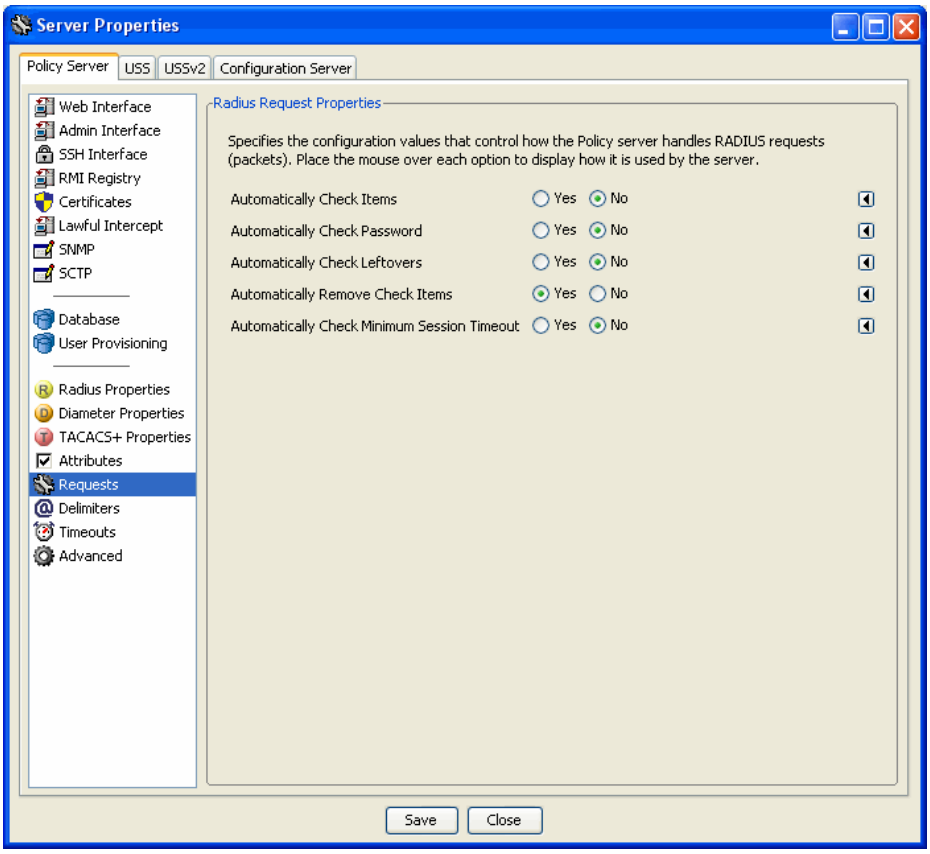
Table 11-3 Attributes Properties

Field	Description	Type	Value
Reveal Hidden Attributes	If enabled, attributes that are marked as hidden in the dictionary are displayed in the packet trace. If disabled, hidden attribute value is displayed as *<hidden>*.	Boolean	Yes No
Strict Attribute Encoding	If enabled, attributes that cannot be encoded cause exception. If not enabled, attributes that cannot be encoded are skipped or are not sent.	Boolean	Yes No

7 Select **Requests**.

Result: The **Radius Request Properties** panel opens.

Figure 11-5 Radius Request Properties



8 Use Table 11-4 to enter the information and click **Save**.

Table 11-4 RADIUS Requests Properties

Field	Description	Type	Value
Automatically Check Items	If enabled, the policy server runs a check item plug-in equivalent at the end of the method chain.	Boolean	Yes No
Automatically Check Passwords	If enabled, the policy server checks the password at the end of the method chain. This property is similar to the AuthLocal plug-in.	Boolean	Yes No
Automatically Check Leftovers	If enabled, the policy server rejects a request if there is Check-Items left to be checked.	Boolean	Yes No
Automatically Remove	If enabled, the policy server removes check items as	Boolean	Yes No

Field	Description	Type	Value
Check Items	they are checked by plug-ins.		
Automatically Check Minimum Session Timeout	If enabled, the policy server compares the minimum session timeout with the Time-of-Day value to decide whether to accept the request.	Boolean	Yes No

Configure delimiters for policy server

Overview

The policy server allows parsing of the User-Name attribute into the Base-Name and Realm attributes. **Realm delimiter characters,** lists all valid delimiters to split the User-Name attribute. All delimiters are evaluated in the order they are entered. User-Name is searched character by character from left to right for the match. The split is done on the first occurrence of the delimiter.

Once a match is found, **Delimiters for realms on the right-hand side** determines which part of the User-Name attribute is the Base-User-Name and which is the Realm.

<domain-name\username> For this case, the delimiter should be "\\".

If you specify a delimiter in the second property that was used to parse the User-Name, it is parsed as <Base-Name>[Delimiter]<Realm>.

By default, the router parses usernames as follows:

username@domainName

The string to the left of the forward slash (/) is the realm name, and the string to the right of the @ symbol is the domain name.

Purpose

Use this procedure to configure the delimiters for the policy server.

Procedure

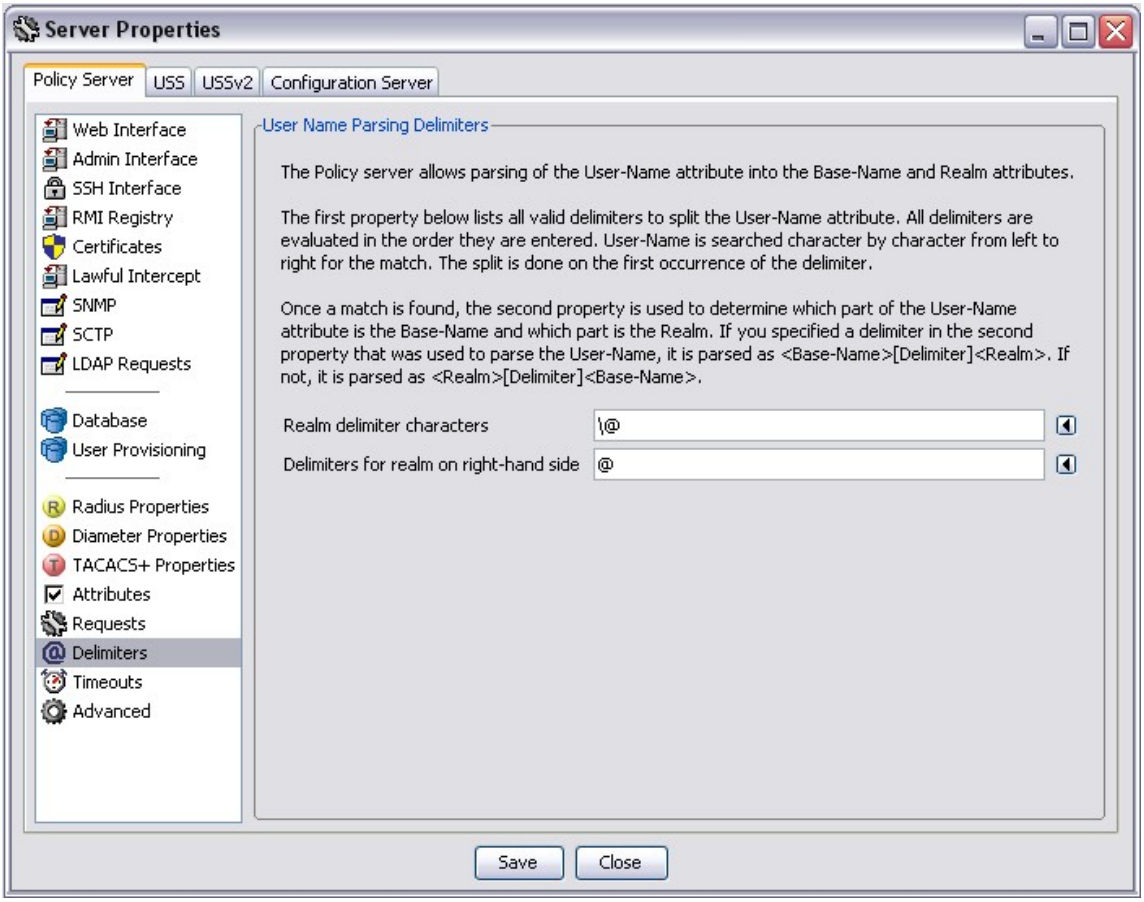
1 From the SMT navigation pane, select **Configuration Tools** -> **Server Properties**.

Result: The **Server Properties** window opens.

2 Select **Policy Server->Delimiters**.

Result: The **User Name Parsing Delimiters** panel opens.

Figure 11-6 User Name Parsing Delimiters


Server Properties
Policy Server
USS
USSv2
Configuration Server
Web Interface
Admin Interface
SSH Interface
RMI Registry
Certificates
Lawful Intercept
SNMP
SCTP
LDAP Requests
Database
User Provisioning
Radius Properties
Diameter Properties
TACACS+ Properties
Attributes
Requests
Delimiters
Timeouts
Advanced
User Name Parsing Delimiters
The Policy server allows parsing of the User-Name attribute into the Base-Name and Realm attributes.
The first property below lists all valid delimiters to split the User-Name attribute. All delimiters are evaluated in the order they are entered. User-Name is searched character by character from left to right for the match. The split is done on the first occurrence of the delimiter.
Once a match is found, the second property is used to determine which part of the User-Name attribute is the Base-Name and which part is the Realm. If you specified a delimiter in the second property that was used to parse the User-Name, it is parsed as <Base-Name>[Delimiter]<Realm>. If not, it is parsed as <Realm>[Delimiter]<Base-Name>.
Realm delimiter characters
\@
Delimiters for realm on right-hand side
@
Save
Close

3 Use Table 11-5 to enter the information and click **Save**.

Table 11-5 User Name Parsing Delimiters

Field	Description	Type	Value
Realm delimiter characters	Enter the realm delimiter characters Specifies a list of characters in search order to parse the user name into a user and realm. By default, the realm is the left-hand value and the user is the right-hand value, unless the delimiter is found in the	Text	Default value: @

Field	Description	Type	Value
	Delimiters for realm on right side value.		
Delimiters for realms on the right-hand side	Enter the delimiters for realms on the right-hand side Specifies that the realm is the right-hand value and the user is the left-hand value of the parsed user name. This list is not a subset of the Realm Delimiter characters.	Text	Default value: @

Result: The configured values are displayed on the **User Name Parsing Delimiters** panel.

Configure timeout properties of policy server

Purpose

Use this procedure to configure timeout properties of policy server.

Procedure

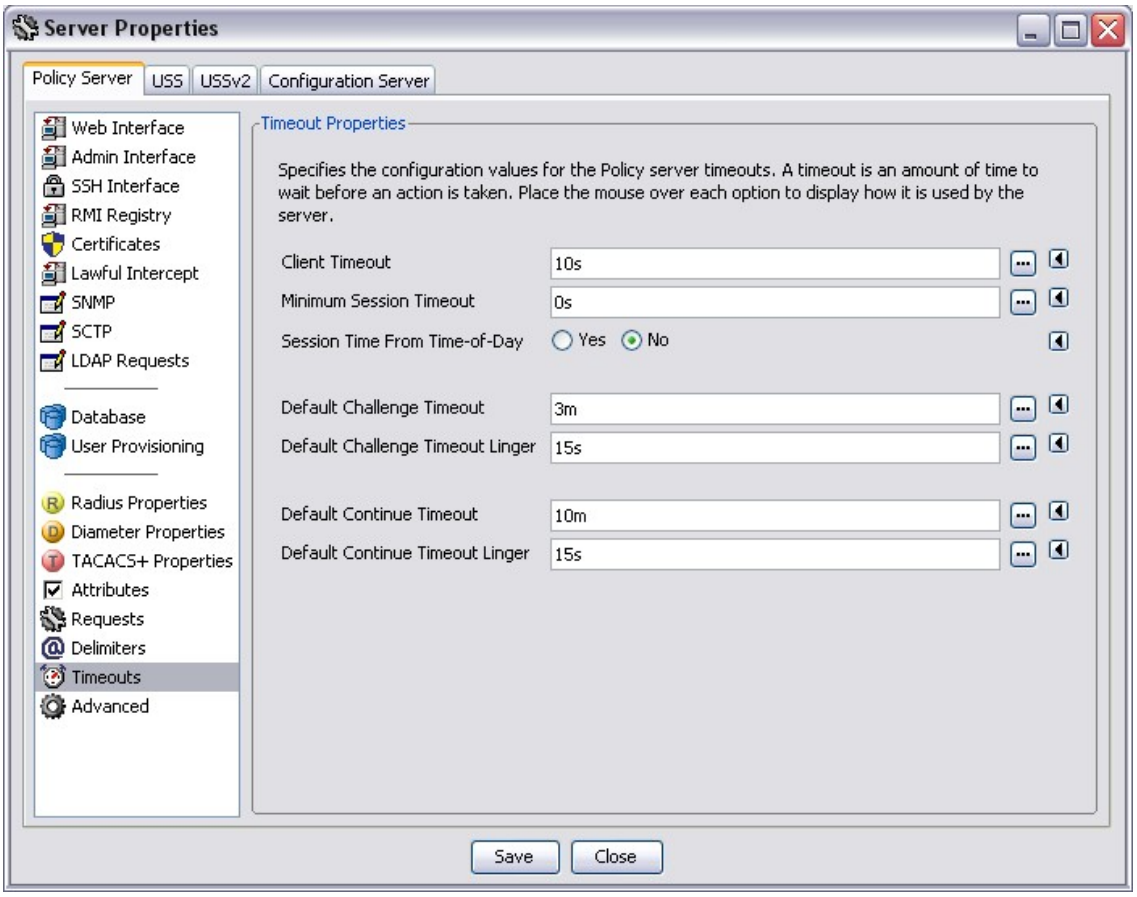
1. From SMT navigation pane, select **Configuration Tools** -> **Server Properties**.

   Result: The **Server Properties** window opens.

2. Select **Timeouts**.

   Result: The **Timeout Properties** panel opens.

Figure 11-7 Timeout Properties



3 Use Table 11-6 to enter the information and click **Save**.

Table 11-6 Timeout Properties

Field	Description	Type	Value
Client Timeout	Enter the time for which the policy server needs to wait before it discards the requests. **Note:** Match the **Client Timeout** with the timeout set on the NAS client.	Use ..., to specify the duration.	Default value: 10 s
Minimum Session Timeout	Enter the minimum session timeout. The policy server rejects any request that has a session-time value less than the value specified.	Use ..., to specify the duration.	Default value: 0 s

Field	Description	Type	Value
	If Session Time is not set in the reply attributes, then no action is needed.		
Session Time from Time-of-Day	If enabled, the session time is the time remaining from the Time-of-Day check item.	Boolean	Yes No
Default Challenge Timeout	Enter the time for which the policy server needs to wait for the challenge response from the clients.	Use , to specify the duration.	Default value: 3 m
Default Challenge Timeout Linger	Enter the time-out before marking the challenge response as Linger.	Use , to specify the duration.	Default value: 15 s
Default Continue Timeout	Enter the time for which the policy server needs to wait for the continue response from the clients.	Use , to specify the duration.	Default value: 10 m
Default Continue Timeout Linger	Enter the time-out before marking the continue response as Linger.	Use , to specify the duration.	Default value: 15 s

Result: The configured values are displayed on the **Timeout Properties** panel.

12 8950 AAA Configuration server

Overview

Purpose

This chapter describes the 8950 AAA configuration server. The configuration server allows remote administration of 8950 AAA. Configuration server allows you to connect to the 8950 AAA server remotely using SMT.

Contents

This chapter covers the following topics.

8950 AAA configuration server	139
Configuration server properties	140

8950 AAA configuration server

8950 AAA SMT is used not only to connect to 8950 AAA server on the local system but also for connecting remotely. Remote connection is achieved by using the configuration server.

You can connect to the 8950 AAA server in a secure mode or in an unsecured mode. If you connect to 8950 AAA server securely, ensure that there is a valid *trusted* certificate.

When you establish a secure connection to the 8950 AAA server through configuration server, the SMT validates the 8950 AAA server using its own trusted certificate. Once the certificate is validated, the connection is established.

There are separate admin interface commands for configuration server.

Configuration server properties

Purpose

Use this procedure to configure the configuration server.

Procedure

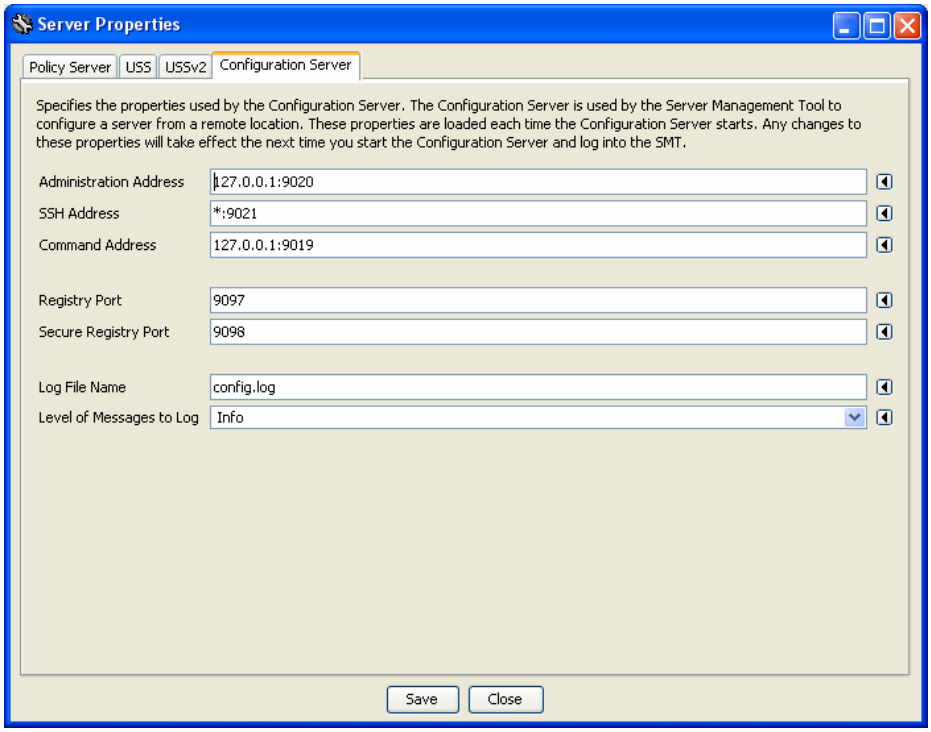
1 From the SMT navigation pane, select **Configuration Tools** -> **Server Properties**.

Result: The **Server Properties** window opens.

2 Click **Configuration Server**.

Result: The **Configuration Server** panel opens.

Figure 12-1 Server Properties


Server Properties
Policy Server
USS
USSv2
Configuration Server
Specifies the properties used by the Configuration Server. The Configuration Server is used by the Server Management Tool to configure a server from a remote location. These properties are loaded each time the Configuration Server starts. Any changes to these properties will take effect the next time you start the Configuration Server and log into the SMT.
Administration Address
127.0.0.1:9020
SSH Address
*:9021
Command Address
127.0.0.1:9019
Registry Port
9097
Secure Registry Port
9098
Log File Name
config.log
Level of Messages to Log
Info
Save
Close

3 Use Table 12-1 to enter the information and click **Save**.

Table 12-1 Configuration Server properties

Field	Description	Type	Value
Administration Address	Enter the TCP/IP address on which the configuration server - admin interface listens for connections. The hostname must be a name that corresponds to a local interface on the machine, or the value "*", which represents all local interfaces.	Network Address in *xxx.xxx.xxx.xxx:port* format	Default value:*.9020.
SSH Address	Enter the address and port that the server listens for SSH connections.	Network Address in *xxx.xxx.xxx.xxx:port* format	Default value:*.9020. Port number 0 implies do not start SSH at all.
Registry Port	Enter the port to be used when creating an RMI registry. Normally, an RMI registry runs at the address specified. However, if there is no registry, the configuration server tries to create one on the local host. By default, it uses the RMI port 9097, but this property enables another port if necessary.	Integer	Default value: 9097
Secure Registry Port	Enter the secure registry port for connecting through RMI secured mode.	Integer	Default value: 9098
Log File Name	Specify the name of the file in which configuration server needs to write the messages and errors.	Text	Default value: *config.log*
Level of Messages to Log	Select the required log level (or debug level). The level determines the type of messages that the configuration server writes to the log file.	One of the list values	Error Warning Notice Info Salient Debug Verbose Blither Default value: Info

Result: The configuration server properties configured are displayed on the **Server Properties** window.

13 Derby database

Overview

Purpose

This chapter provides procedures to configure and access Derby using SMT. For enterprise networks with a small subscriber database, 8950 AAA provides embedded Derby database.

Contents

This chapter covers the following topics.

Database configuration	143
Configure DB replication	145

Database configuration

Purpose

Use this procedure to configure the built-in Derby database.

When to use

Specify the configuration value for the built-in Derby database. Use this procedure if the default value needs to be changed.

Procedure

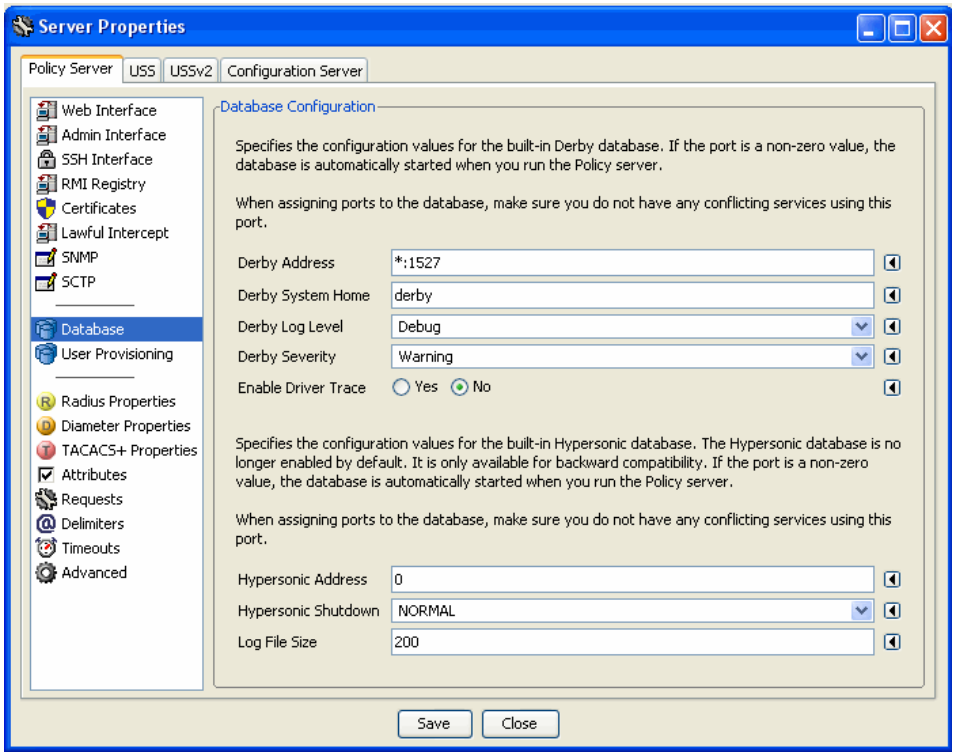
1 From SMT navigation pane, select **Configuration Tools -> Server Properties**.

Result: The **Server Properties** window opens.

2 Select **Policy Server -> Database**.

Result: **Database Configuration** panel opens.

Figure 13-1 Server Properties



3 Use Table 13-1 to enter the Derby DB information and click **Save**.

Table 13-1 Database Configuration

Field	Description	Type	Value
Derby Address	Set the listen addresses for Apache Derby database server. **Note:** If the port is non-zero value, the database automatically starts when you run the policy server. **Important!** When assigning ports to the database, ensure that no other conflicting services are using the port.	Network address in *xxx.xxx.xxx.xxx:<port>* format	The default value: *:1527

Field	Description	Type	Value
Derby System Home	• Sets the location of the Derby database files. • Specifies the name of subdirectory under the 8950 AAA base installation directory. • Sets the *derby.system.home* Derby property.	Text	The default value: derby
Derby Log Level	Sets the 8950 AAA log level that messages from the Derby database server are logged.	One of the list value	Warning Notice Info Salient Debug Verbose Blither Never The default value: Debug
Derby Severity	Set the level of the Derby messages that Derby sends to the logging system. These messages are logged at the Derby log level in the AAA logging system.	One of the list value	None Warning Statement Transaction Session Database System
Enable Driver Trace	If enabled, the Derby driver level messages are logged in the policy server log.	Boolean	Yes No The default value: No

Configure DB replication

Purpose

Use this procedure to configure the Derby replication.

Note: To create a database use the Admin interface command *derby create*.

When to use

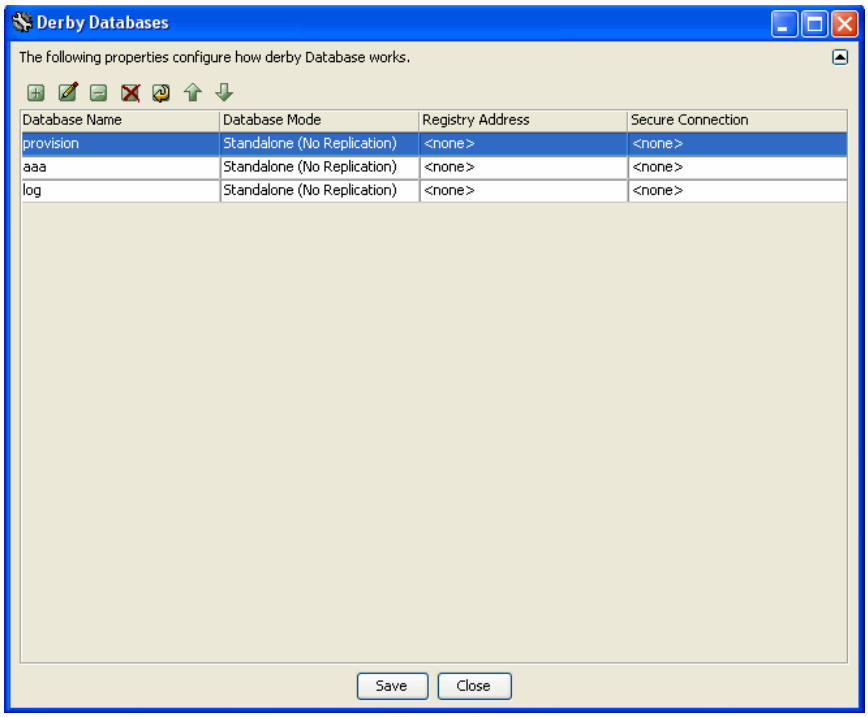
When you want to create a database configuration or modify an existing database configuration to enable the Derby replication.

Procedure

1 From SMT navigation pane, select **Configuration Tools -> Derby Databases**.

Result: The **Derby Databases** window opens. This window displays the predefined databases.

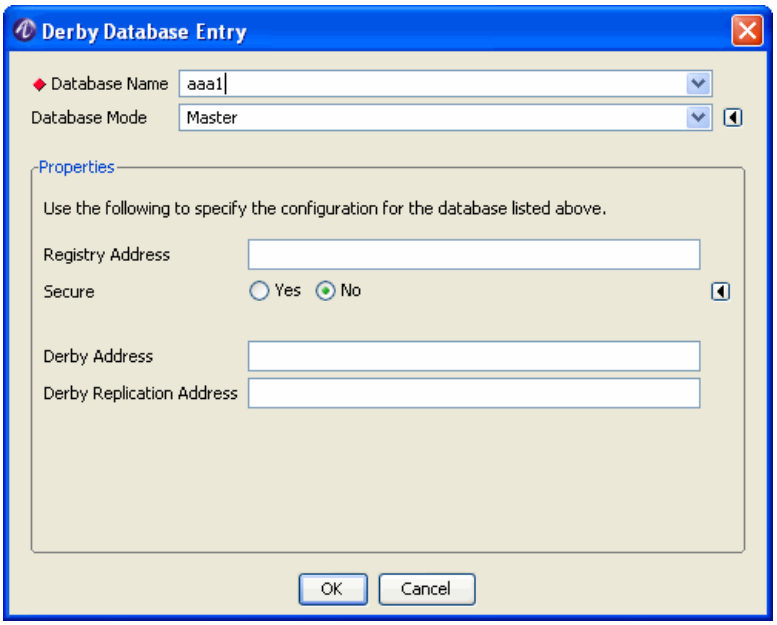
Figure 13-2 Derby Databases



2 Click .

Result: The **Derby Database Entry** window opens.

Figure 13-3 Derby Database Entry



3 Use Table 13-2 and Table 13-3 to enter the values for the fields and click **OK**.

Table 13-2 Derby Database Entry

Field	Description	Type	Value
Database Name	Enter the database name	Text	-
Database Mode	Select the required mode of database configuration. Database is configured in one of the following mode: • On a non-replication mode • To be a master in replication mode. In this mode, the database is in an active state and modified entries are replicated to the secondary server. • To be slave in replication mode. In this mode, the database is configured in slave mode and is a read-only database. **Note:** You can read slave data only if master database is down	One of the list values	• Standalone (No Replication) • Master • Slave (Read Only)

Table 13-3 Database Properties

Field	Description	Type	Value
Registry Address	Enter the RMI registry address. If the master database is configured in replication mode, enter the IP address of the slave. If the slave database is configured in replication mode, enter the IP address of the master. Master updates the slave database, hence the master registers the slave address. When master goes down, slave can be accessed in a read-only mode. Slave must know which master it responds to, hence registers the master address. **Note:** When master goes down, slave cannot update the database; it can only read from the database.	Network address in *xxx.xxx.xxx.xxx:<port>* format	The default port for secure connection is 9100 or 9099
Secure	Specify whether the communication is to be secure or not.	Boolean	• Yes • No Default value: No
Derby Address	Enter the address of Apache Derby database where slave is configured. If master database is configured in replication mode, then this address points to the IP address of the slave. This property is disabled for slave configuration because, if the master goes down, the slave can only read the data and cannot update.	Network address in *xxx.xxx.xxx.xxx:<port>* format	Default port: 1527
Derby Replication Address	Enter the Derby Replication address. Specifies the address of the system where the Master	Network address in *xxx.xxx.xxx.xxx:<port>* format	Default port: 4851

Field	Description	Type	Value
	replicates to (the Slave). If Master database is being configured in replication, then this address points to the IP address of the slave. This property is disabled for slave configuration, as it has the replicated copy		

4 **Result:** The new database is displayed on the **Derby Database** window.

Part V: 8950 AAA management

Overview

Purpose

The SMT provides various tools to manage the 8950 AAA server, locally and remotely. This part provides a description of few management tools and procedures used in the 8950 AAA server in the enterprise network. For more details, see http://www.8950aaa.com/doc/6.3/SMT.pdf

This part covers the following chapters.

Remote configuration	153
Certificate management	165

14 Remote configuration

Overview

Purpose

This chapter describes the 8950 AAA remote configuration.

Contents

This chapter covers the following topics.

8950 AAA remote configuration	153
Configure server entry	155
Add file list	158
Edit file list	163
Delete file entry	163

8950 AAA remote configuration

Remote configuration allows retrieval of files from a remote server using configuration server. Remote configuration provides a centralized location for configuration files.

An 8950 AAA machine, which provides centralized location for configuration files, acts as a master machine.

Another 8950 AAA machine, which tries to retrieve the configuration files from the master system, becomes the slave.

The master configures the IP address of all the slaves, and the slave configures the information of the master, for example, the IP address.

Slave retrieves the files, which require a centralized storage, from the master machine. Retrieval of files requires the policy server to be active on the slave machine.

When a file is updated or modified on the master machine, master copies the updated file to the respective client machines (if the file is present in the files list of client) through notification.

For the slave to receive the copy of modified files during notification (notify action), the policy server needs to be active on the slave machine.

The configuration server needs to be running on the master machine every time.

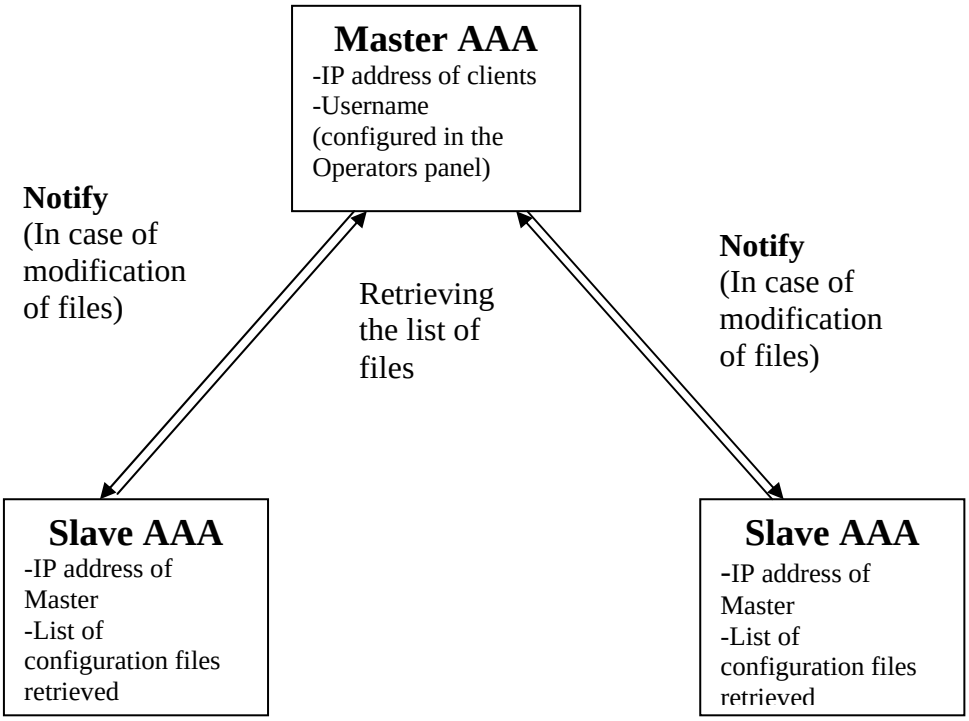
Note: There is no limit on the size of the file transferred.

A common password is configured on the **Operators** panel of master and slave machine with appropriate file access permissions. The password has to be in plain text (not encrypted).

Following are the types of configuration files transferred between the master and the slave machine:

- Critical files – The critical files are files that the policy server reads before processing the remote configuration. If critical files are retrieved remotely, then the server needs to restart (automatically) to receive the changes from the remote server. The following are the critical files:
  - server properties
  - remote_config.html
  - security properties
  - dictionary.xml
- Non-critical files - Files which do not affect the policy server hence, policy server need not be restarted upon modification of these files. Figure 14-1 8950 AAA remote configuration illustrates the 8950 AAA remote configuration scenario.

Figure 14-1 8950 AAA remote configuration



Configure server entry

Purpose

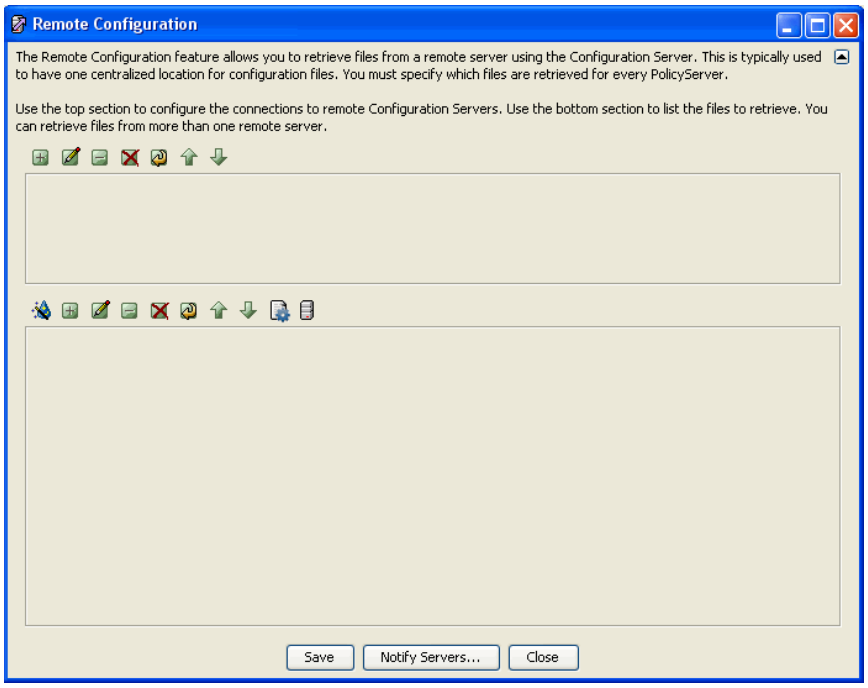
Use this procedure to configure the server entries. Master configures the slave information and slave configures the master information.

Procedure

1 From SMT navigation pane, select **Configuration Tools -> Remote Configuration**.

Result: The **Remote Configuration** window opens. See Figure 14-2.

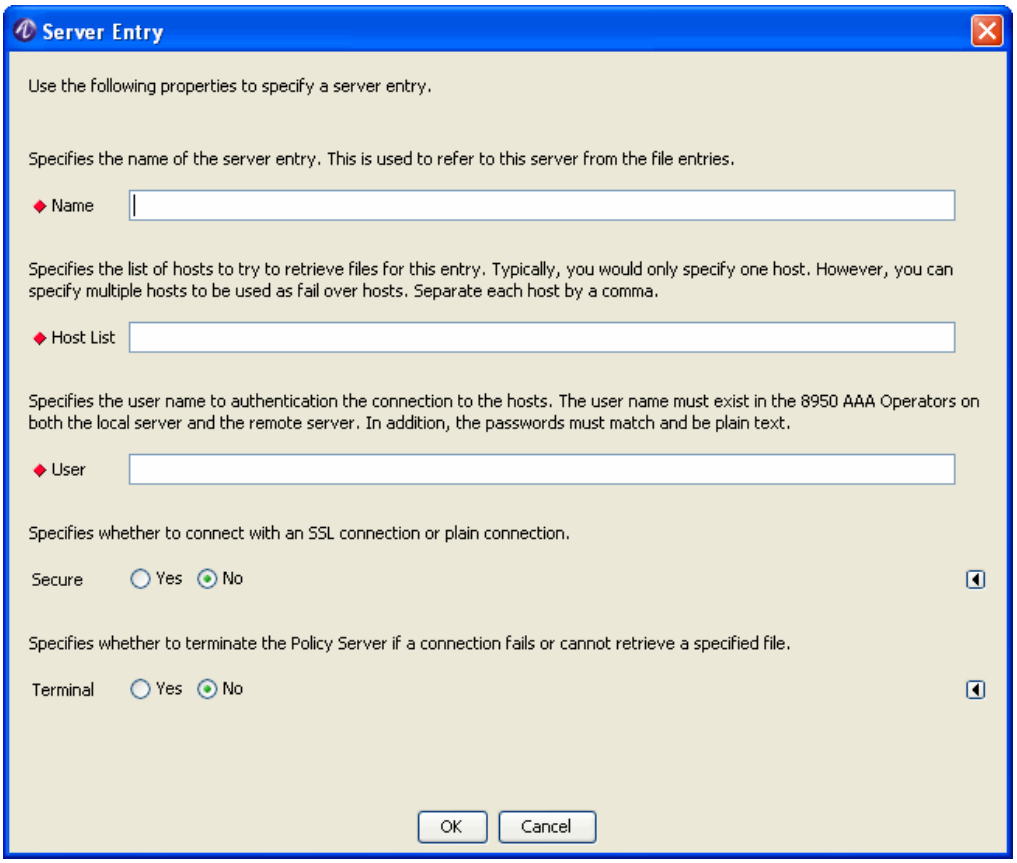
Figure 14-2 Remote Configuration


Remote Configuration
The Remote Configuration feature allows you to retrieve files from a remote server using the Configuration Server. This is typically used to have one centralized location for configuration files. You must specify which files are retrieved for every PolicyServer.
Use the top section to configure the connections to remote Configuration Servers. Use the bottom section to list the files to retrieve. You can retrieve files from more than one remote server.
Save
Notify Servers...
Close

2 From the top panel, click .

Result: The **Server Entry** window opens. See Figure 14-3.

Figure 14-3 Server Entry


Server Entry
Use the following properties to specify a server entry.
Specifies the name of the server entry. This is used to refer to this server from the file entries.
Name
Specifies the list of hosts to try to retrieve files for this entry. Typically, you would only specify one host. However, you can specify multiple hosts to be used as fail over hosts. Separate each host by a comma.
Host List
Specifies the user name to authentication the connection to the hosts. The user name must exist in the 8950 AAA Operators on both the local server and the remote server. In addition, the passwords must match and be plain text.
User
Specifies whether to connect with an SSL connection or plain connection.
Secure Yes No
Specifies whether to terminate the Policy Server if a connection fails or cannot retrieve a specified file.
Terminal Yes No
OK
Cancel

3 Use Table 14-1 to enter the information and click **OK**.

Table 14-1 Server Entry

Field	Description	Type	Value
Name	Enter the name of the server entry. Use this name to refer to the server from file entries.	Text	-
Host List	Enter the host IP address. Specifies the host to try to retrieve files for this entry. **Note:** You can specify multiple hosts to be used as fail over hosts, which are separated by a comma. If the first specified host fails to connect, second one is tried, and so on.	Network IP address format: *xxx.xxx.xxx.xxx.<port>*	-
User	Enter the user name to authenticate the connection to		

Field	Description	Type	Value
	the hosts. **Important!** The user name exists in the 8950 AAA Operators on both the local server and the remote server. The passwords must match and be plain text.		
Secure	Specify whether to connect with an SSL connection or plain connection.	Boolean	Yes No
Terminal	Specify whether to terminate the policy server during the following conditions: Connection failure Fail to retrieve the specified file	Boolean	Yes No

Result: The configured values are displayed in the **Server Entry** window.

Add file list

Purpose

Use this procedure to add the list of file to retrieve from the master machine.

Note: This procedure is not required on a master system.

Procedure1

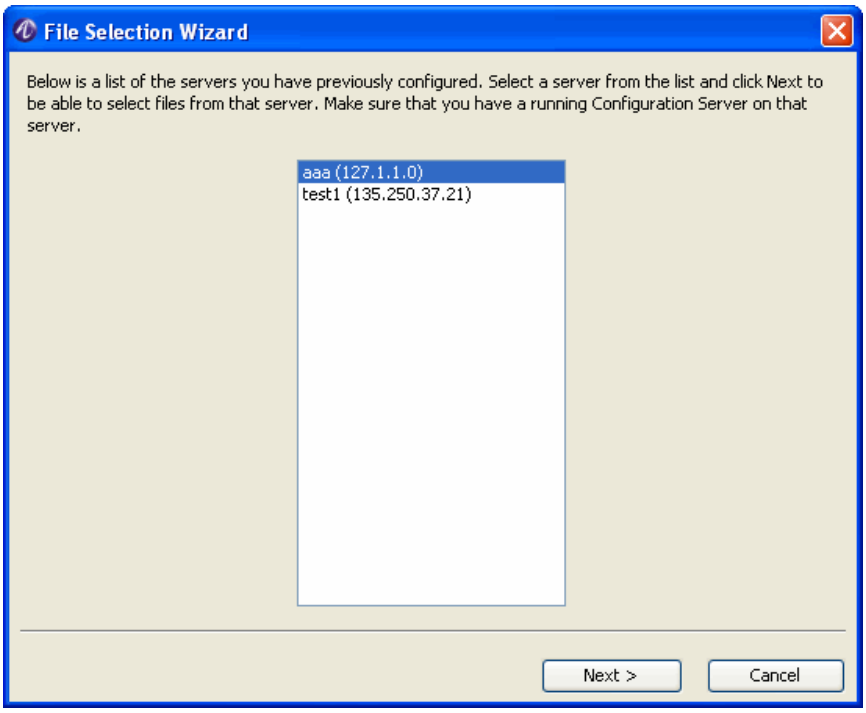
1 From SMT navigation pane, select **Configuration Tools -> Remote Configuration**.

Result: The **Remote Configuration** window opens. See Figure 14-2.

2 From the bottom panel, click .

Result: The **File Selection Wizard** window opens.

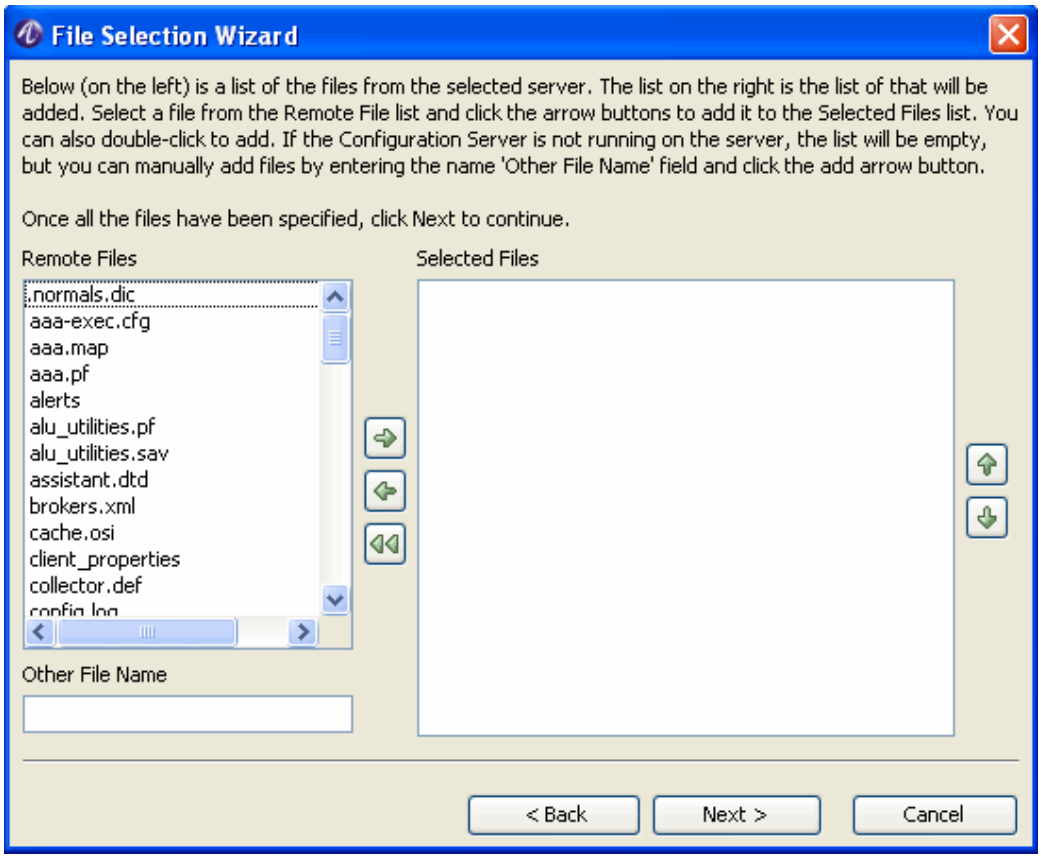
Figure 14-4 File Selection Wizard


File Selection Wizard
Below is a list of the servers you have previously configured. Select a server from the list and click Next to be able to select files from that server. Make sure that you have a running Configuration Server on that server.
aaa (127.1.1.0)
test1 (135.250.37.21)
Next >
Cancel

3 Select the required host from the list and click **Next**.

Result: The **File Selection Wizard** window with the list of files to be selected opens.

Figure 14-5 File Selection Wizard


File Selection Wizard
Below (on the left) is a list of the files from the selected server. The list on the right is the list of that will be added. Select a file from the Remote File list and click the arrow buttons to add it to the Selected Files list. You can also double-click to add. If the Configuration Server is not running on the server, the list will be empty, but you can manually add files by entering the name 'Other File Name' field and click the add arrow button.
Once all the files have been specified, click Next to continue.
Remote Files
Selected Files
.normals.dic
aaa-exec.cfg
aaa.map
aaa.pf
alerts
alu_utilities.pf
alu_utilities.sav
assistant.dtd
brokers.xml
cache.osi
client_properties
collector.def
Other File Name
< Back
Next >
Cancel

4 Perform the following:

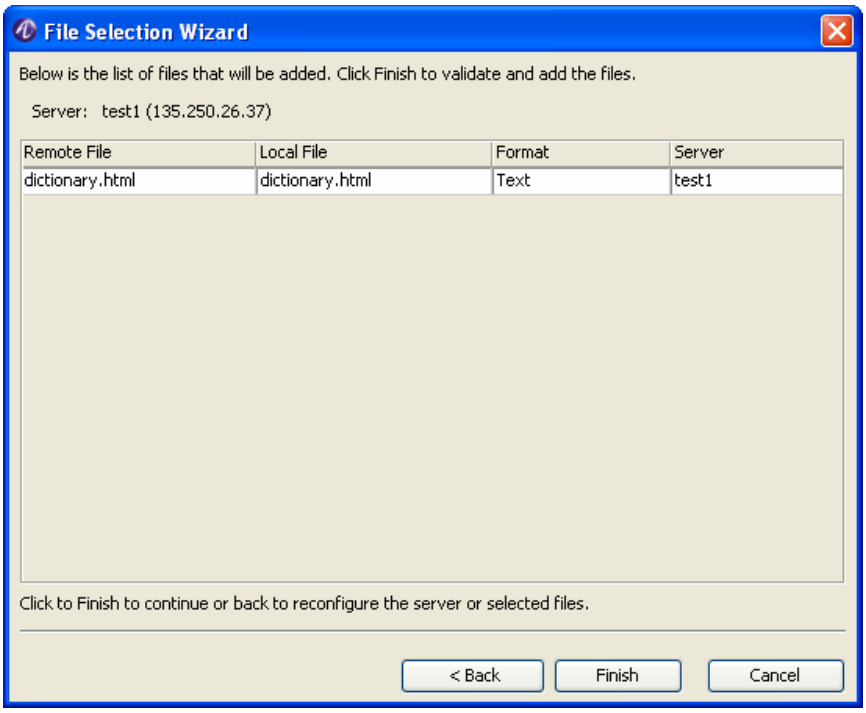
a. Select the required file from the **Remote Files** list. If the required file is not present in the list, enter the file name in the **Other File Name** field.

b. Click to move the selected file to Selected File list.

c. Click **Next**.

Result: The **File Selection Wizard** window with the selected file details opens.

Figure 14-6 File Selection Wizard – Selected file details



5 Click **Finish**.

Result: The selected list of files appears on the **Remote Configuration** window.

Procedure2

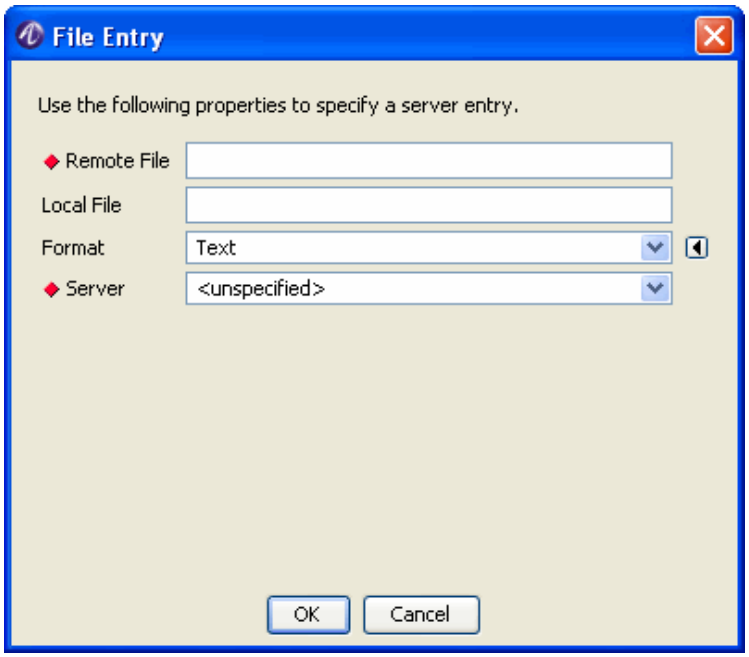
1 From SMT navigation pane, select **Configuration Tools -> Remote Configuration**.

Result: The **Remote Configuration** window opens. See Figure 14-2.

2 From the bottom panel, click .

Result: The **File Entry** window opens.

Figure 14-7 File Entry



3 Enter the information using the **File Entry** table and click **OK**.

Table 14-2 File Entry

Field	Description	Type	Value
Remote File	Enter the name of the file to retrieve from the remote server.	Text	-
Local File	Enter the file name to save locally which is retrieved from remote machine. If not specified, the remote file with the same name is saved.	Text	-
Format	Select the required file format. Select **Text** for plain text files and **Binary** for zip files.	One of the list values	Text Binary
Server	Specify the required host name.	Text	-

Result: The configured values are displayed on the **Remote Configuration** window.

Edit file list

Purpose

Use this procedure to edit a file entry.

Procedure

1 From SMT navigation pane, select **Configuration Tools -> Remote Configuration**.

Result: The **Remote Configuration** window opens. See Figure 14-2.

2 Select the required file entry and click .

Note: Click to create a copy of the selected file.

Note: Click to change the file format of the selected file and click to change the host server.

Result: The **File Entry** window opens. See Figure 14-7.

3 Use Table 1-1 to edit the required field and click **OK**.

Result: The changes are displayed on the **Remote Configuration** window.

Delete file entry

Purpose

Use this procedure to delete a file entry.

Procedure

1 From SMT navigation pane, select **Configuration Tools -> Remote Configuration**.

Result: The **Remote Configuration** window opens. See Figure 14-1.

2 Select the required file entry and click .

Note: To delete all the files, click .

Result: The selected file entry is deleted.

15 Certificate management

Overview

Purpose

This chapter provides an overview about certificate management. It describes what is a digital certificate and the various types of digital certificates used in the 8950 AAA configuration. This chapter also provides procedures to manage certificates, for example, procedure to request for a certificate, procedure to view a certificate, procedure to create a certificate, and so on.

Authentication methods such as EAP-PEAP, EAP-TTLS and EAP-TLS are commonly used in an enterprise network. These methods use the X.509 certificates for authentication.

Contents

This chapter covers the following topics.

Certificates	165
8950 AAA and certificates	168
Generate certificates for AAA using third-party CA	169

Certificates

Need for certificates

Network authentication using EAP-TLS, EAP-TTLS and EAP-PEAP involves X.509 digital certificates. Using these authentication methods, supplicants or end-user devices can verify the server credentials and as an option, the server can verify the credentials of the supplicants or end-user devices.

X.509 Certificates are issued by the Certificate Authority (CA) and are used in encrypting the data that is sent over the wire.

Encryption/Decryption using Digital certificates

Asymmetric cryptography is also known as public-key cryptography, which involves a pair of private and public keys to encrypt the data.

Public keys are incorporated into a certificate. They are distributed with software or by electronic means, such as web sites, information servers, and so on, and need not be protected from disclosure.

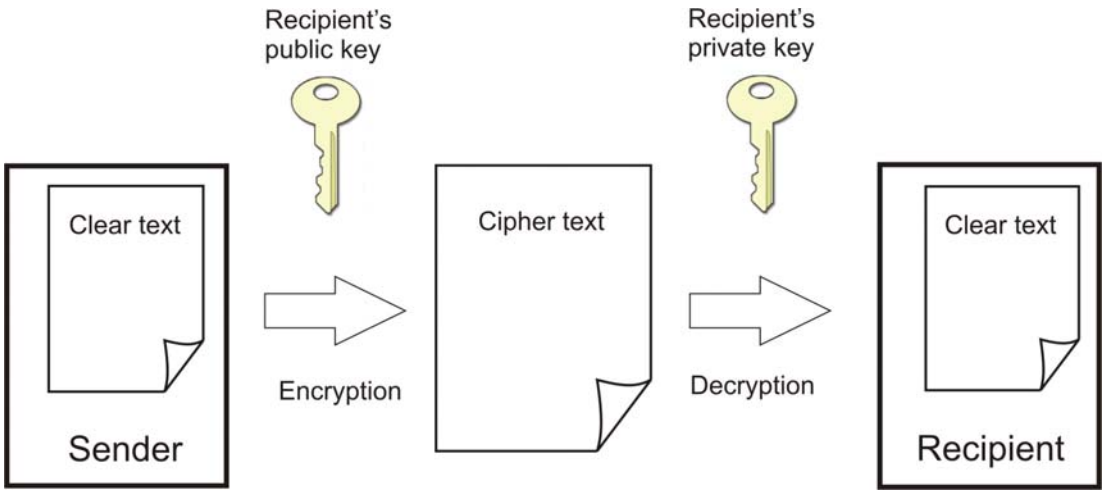
The owners must safeguard all private keys against compromise, and keep the private key a secret.

A digital certificate is a public key associated with an element. The element can be a person, device, web server, and so on, and carries the fingerprint of the CA. In other words, a digital certificate is digitally signed with the CA private key and carries validity dates and a serial number. As extra elements, the certificate carries extra information, such as key usage and constraints on the possible use of the certificate.

Data encrypted with the private key can only be decrypted with its public key, and the inverse is true.

If the data sent by the sender is encrypted with the public key of the recipient, the data is said to be truly encrypted. The recipient has the private key and can decrypt the message.

Figure 15-1 Encryption and decryption with recipient keys

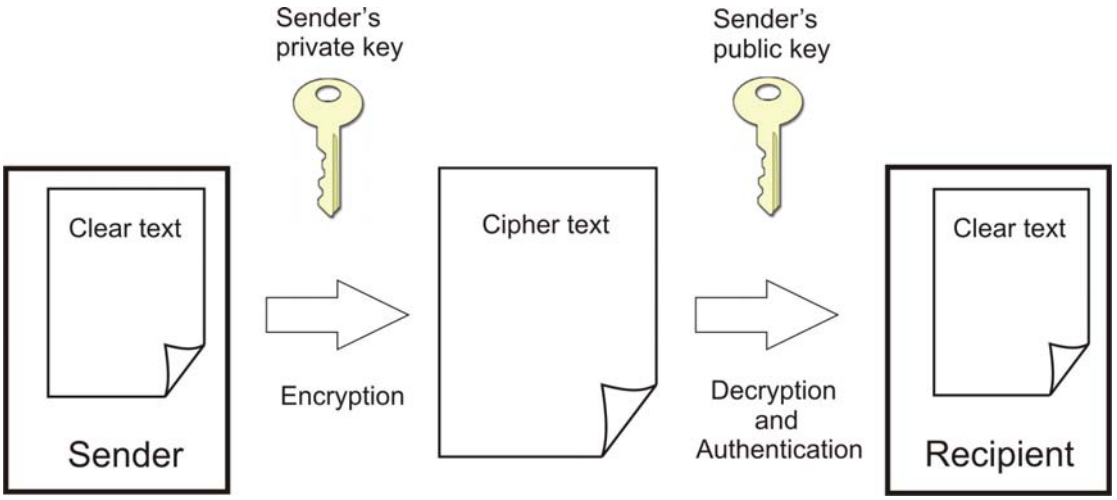


There are two possible ways for the sender to obtain the public key of the recipient:

1. The recipient sends it to the sender in the clear. As it is a public key, there is no risk by sending it on the open.
2. The sender retrieves it from a publicly known storage place, typically provided by a PKI.

In another scenario, the text is encrypted using the private key of the sender, and then any person with the sender's public key can decrypt the message.

Figure 15-2 Encryption and decryption with sender keys

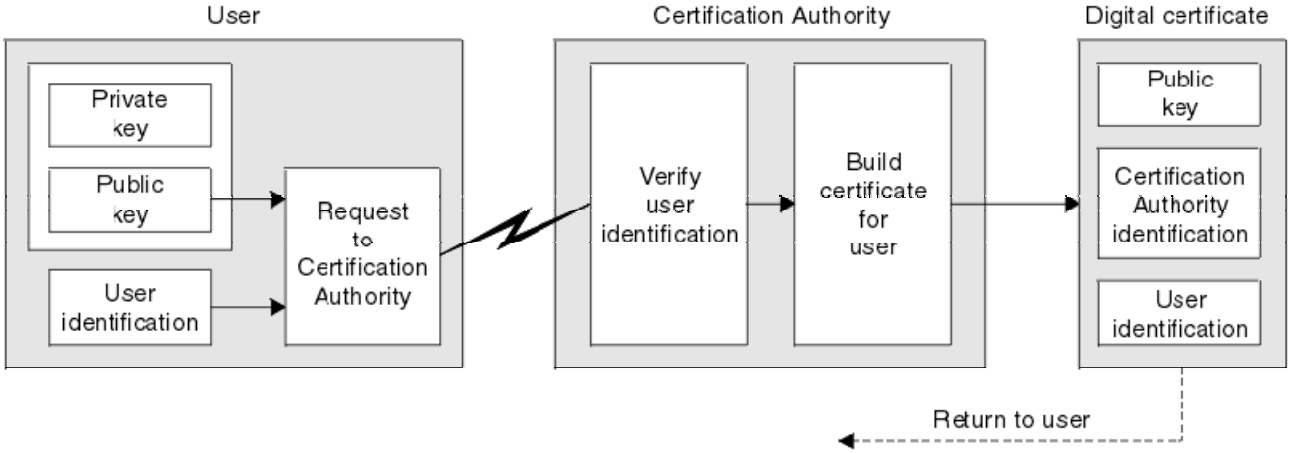


If a recipient is able to decrypt the message, it means the sender owns the other private key pair. Since the sender owns the private key, the recipient is aware of the identity of the sender.

Process to procure the digital certificate

This procedure describes the steps taken by the end user to procure a digital certificate from a trusted CA.

Figure 15-3 Digital Certificate



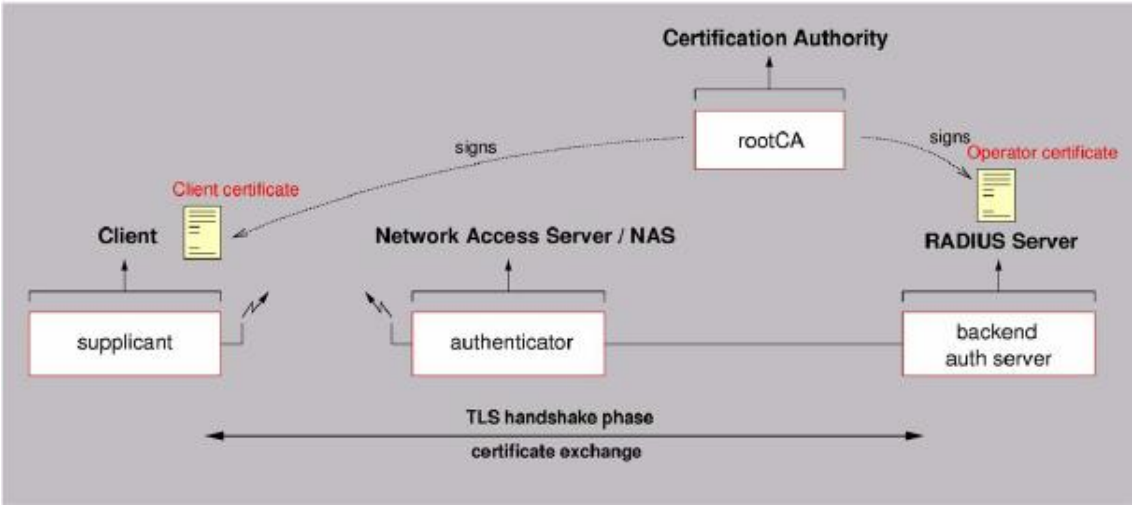
1. The user generates a certificate request and sends it to a CA. This is also known as Root CA.
2. The CA verifies the identity of the user and generates the certificate for the user. This certificate can be a Sub-CA certificate or end user certificate. The end users can act as a Sub-CA and generate further certificates for other entities, or for their own usage.

3 End user certificate file contains the chain of certificates from Root CA, Sub-CAs and the end user certificate.

Certificate deployment on 8950 AAA

In the enterprise network, along with the operator certificates, the 8950 AAA also has the root or trusted certificates of the client. Similarly, the client installs the root or trusted certificate of the server. These root or trusted certificates are used for mutual verification.

Figure 15-4 Deployment on 8950 AAA server



Role of Certificate Manager

A Certificate Manager functions as a root or subordinate certificate authority. This subsystem issues, renews and revokes certificates, and generates Certificate Revocation List (CRLs). The certificate manager publishes certificates to a LDAP directory and files, and CRLs to an LDAP directory or a file. The Certificate Manager is configured to accept requests from end entities, Registration Managers, or both. The certificate manager can process requests either manually (that is, with the aid of a human being) or automatically (based entirely on customizable policies and procedures). When set up to work with a separate Registration Manager, the Certificate Manager processes requests and returns the signed certificates to the Registration Manager for distribution to the end entities.

8950 AAA and certificates

8950 AAA does not issue any certificates. An external Certificate Authority (CA) issues the certificates. The 8950 AAA checks the certificates as part of the authentication process.

Microsoft CA is used in Enterprise environment, although 8950 AAA can use other third-party CAs.

The 8950 AAA server is provisioned with its certificate chain and private key associated with its server certificate. The 8950 AAA has a complete list of device root certificates that it encounters.

Following are the steps to establish a secure network connection:

The device or client requests for a network connection to the server.

1. The 8950 AAA server responds to the request by sending the server certificate.
2. The device or client verifies the server certificate to confirm that the device is talking to the right server.
3. The device or client validation by 8950 AAA server depends on the configuration mode. 8950 AAA is configured to one of the following modes:
   - **Optional** - The client validation is performed only when the client sends the client certificate.
   - **Required** - The client sends a valid client certificate to get authenticated.
   - **Disabled** - The client validation does not happen.
4. The network connection is established.

Generate certificates for AAA using third-party CA

This procedure describes the configuration of 8950 AAA with certificates issued from third-party CA using the Microsoft CA as an example.

Purpose

Use this procedure to request a certificate from the Microsoft Certificate Services using web server.

Note: The 8950 AAA server is not a certification authority and hence, does not provide certificates. Use these self-signed certificates for testing and demonstration purposes only. Contact the authorized third-party CAs to obtain certificates for production purposes. If you are using Active Directory, use the Microsoft Certificate Services to generate an SSL certificate.

Additional information

To issue a certificate for a web server, ensure that the following items are present:

- Domain administrator account
- Internet Explorer browser
- Windows server installed with Microsoft Certificate Services.

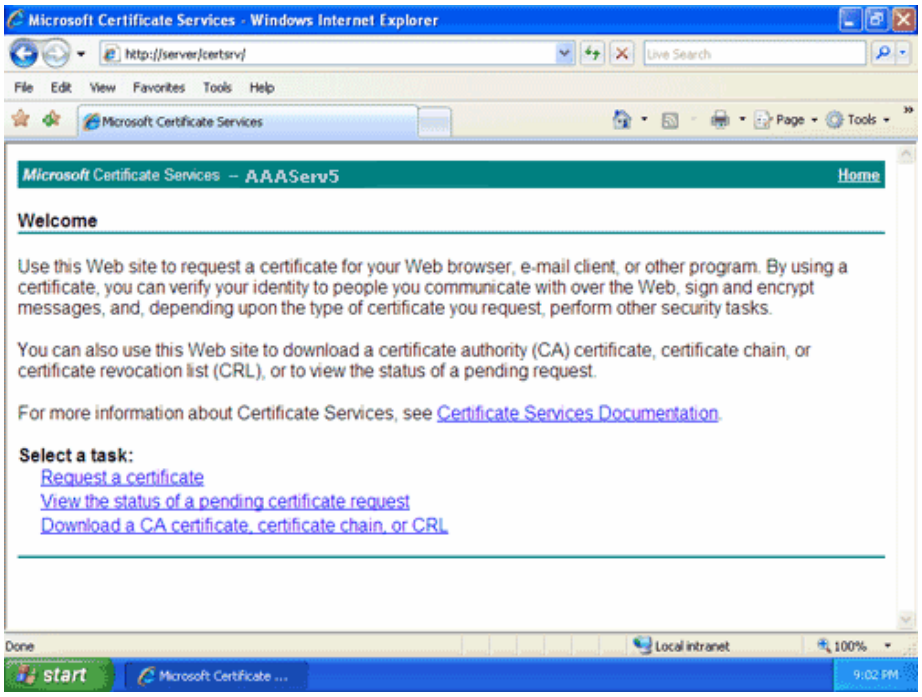
Procedure

Note: Keep the **Certificate Manager** window open until you execute all the steps.

1 Launch the Internet Explorer and type *http://<hostname>/certsrv*, to connect to the *Certificate Services* server.

Result: The **Microsoft Certificate Services** window opens.

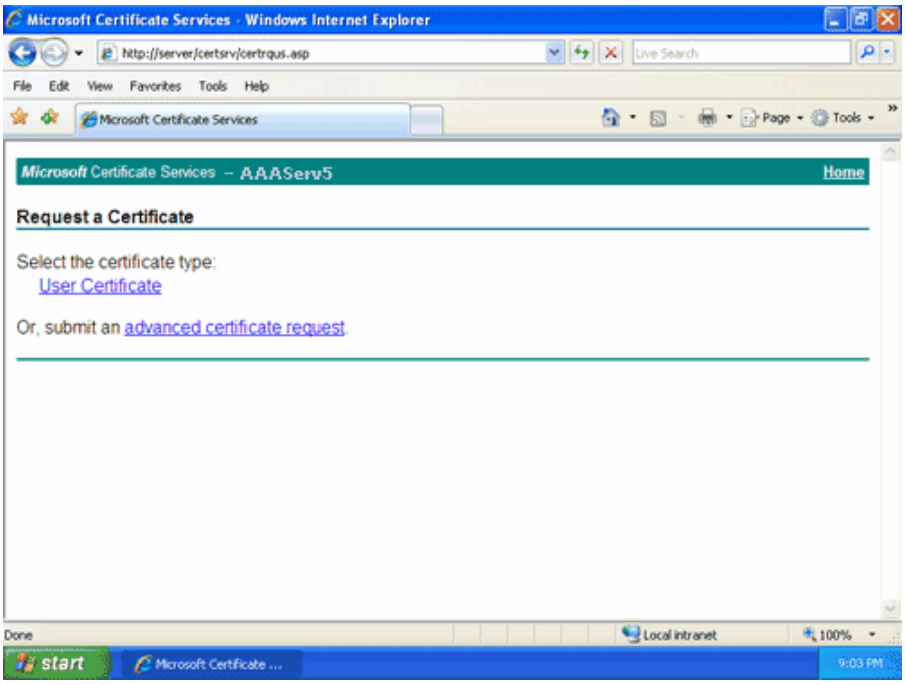
Figure 15-5 Microsoft Certificate Services


Microsoft Certificate Services - Windows Internet Explorer
http://server/certsrv/
File Edit View Favorites Tools Help
Microsoft Certificate Services
Page Tools
Microsoft Certificate Services -- AAAServ5
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Certificate Services, see Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL
Done
Local intranet
100%
start
Microsoft Certificate ...
9:02 PM

2 Click *Request a Certificate* link.

Result: The **Request a Certificate** page opens.

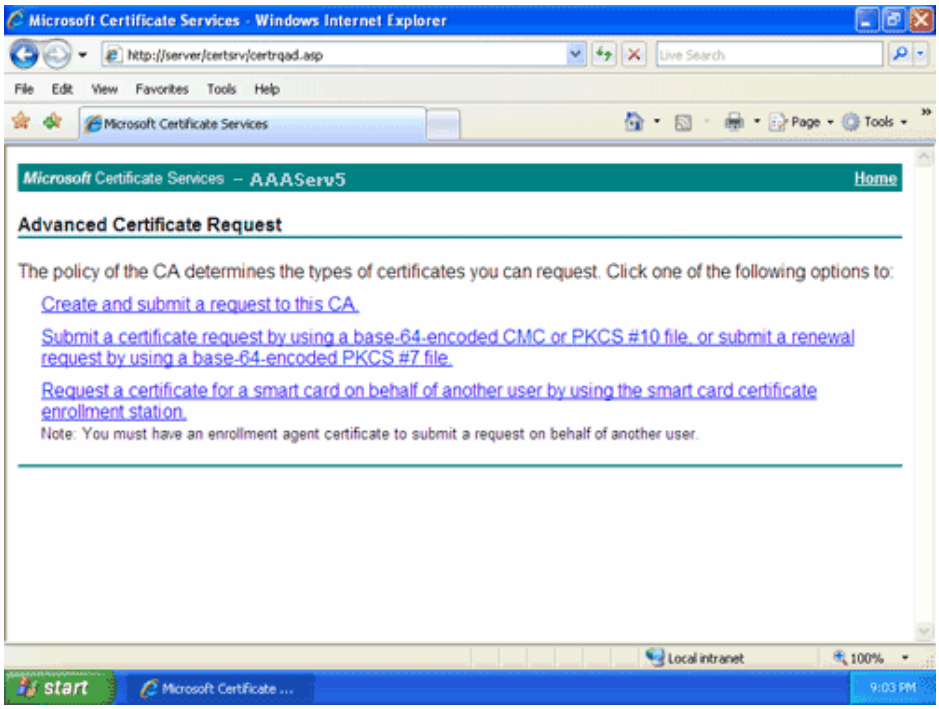
Figure 15-6 Request a Certificate



3 Click *Advanced Certificate Request* link.

Result: The **Advanced Certificate Request** page opens.

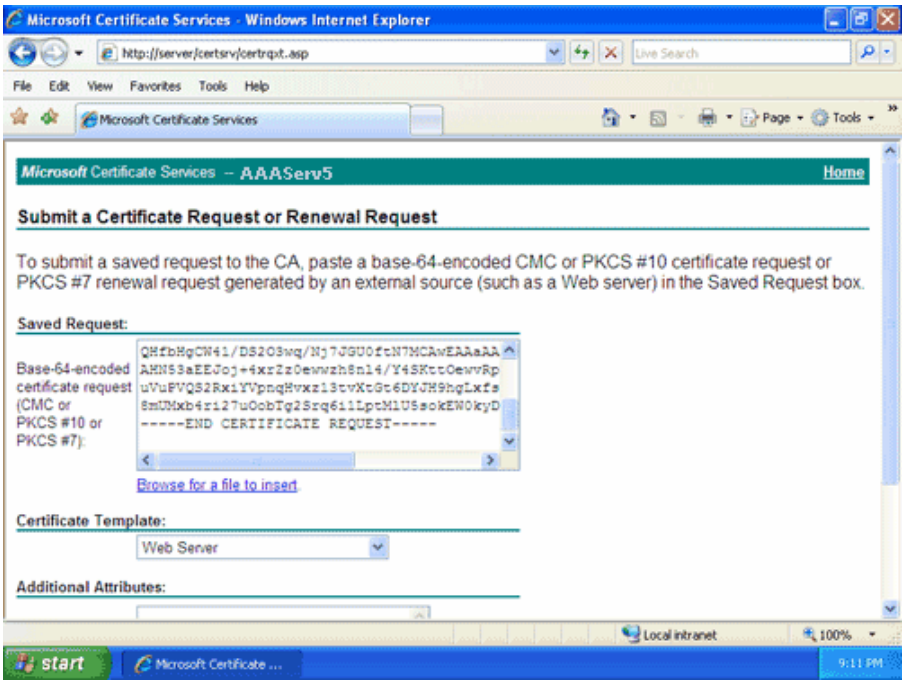
Figure 15-7 Advanced Certificate Request


Microsoft Certificate Services - Windows Internet Explorer
http://server/certsrv/certrqad.asp
File Edit View Favorites Tools Help
Microsoft Certificate Services
Page Tools
Microsoft Certificate Services -- AAAServ5
Home
Advanced Certificate Request
The policy of the CA determines the types of certificates you can request. Click one of the following options to:
Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.
Local intranet
100%
start
Microsoft Certificate ...
9:03 PM

4 Click *Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file or submit a renewal request by using a base-64-encoded PKCS#7 file* link.

Result: The **Submit a Certificate Request or Renewal Request** page opens.

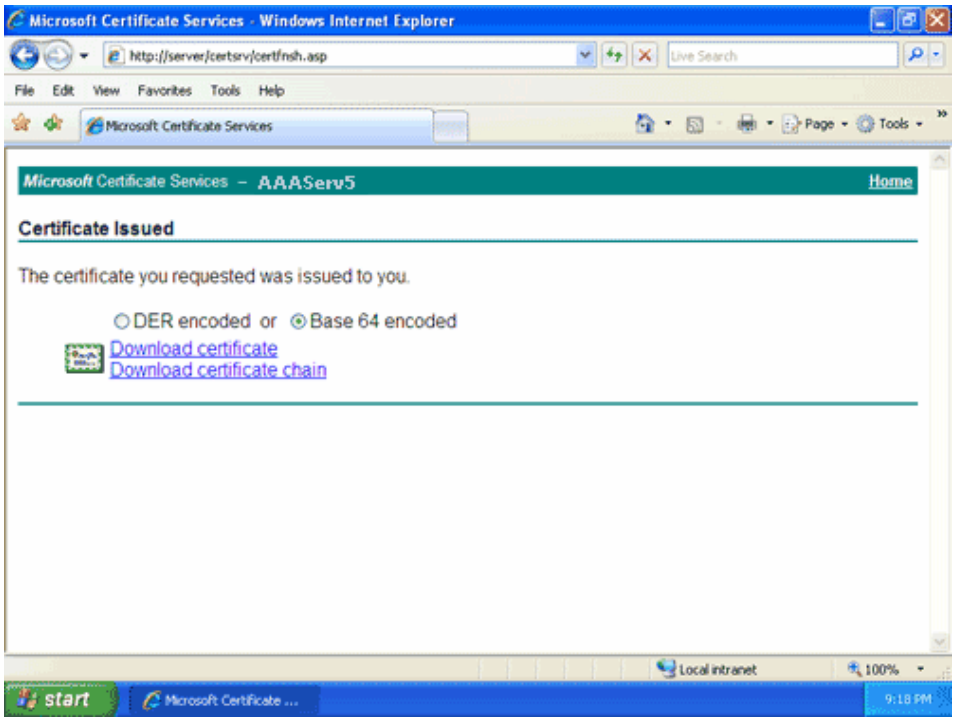
Figure 15-8 Submit a Certificate Request or Renewal Request


Microsoft Certificate Services - Windows Internet Explorer
http://server/certsrv/certrqxt.asp
File Edit View Favorites Tools Help
Microsoft Certificate Services
Page Tools
Microsoft Certificate Services -- AAAServ5
Home
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.
Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
QHfbHgCW41/DS2O3wq/Nj7JGU0ftN7MCAwEAAaAA
AHN53aEEJoj+4xrZz0ewwzh8nl4/Y4SKttOewvRp
uVuPVQS2RxiYVpnqHvxz13tvXtGt6DYJH9hgLxfs
8mUMxb4r127uOobTg2Srq611LptM1U5sokEW0kyD
-----END CERTIFICATE REQUEST-----
Browse for a file to insert.
Certificate Template:
Web Server
Additional Attributes:
Local intranet
100%
start
Microsoft Certificate ...
9:11 PM

5 Copy the certificate information from the **Certificate Info** section and paste in the **Base-64-encoded certificate request** field of Figure 15-8. Select **Web Server** from the **Certificate Template** drop-down list, and click **Submit**.

Result: The **Certificate Issued** page opens.

Figure 15-9 Certificate Issued



6 Select **Base 64 encoded** and click *Download certificate* link.

7 Save the certificate as server in the ..*AAA**run* directory. In the **Certificate Issued** page, click **Home**.

Result: The **Welcome** page appears.

8 Perform the following:

a. Select the **Download a CA Certificate or CRL** and click **Next**.

b. Select **Base 64 Encoded** and click **Download CA Certificate**.

c. Give the filename as *ca* and save to the ..*AAA**run* directory.

Result: The certificate downloads.

Note: Ensure that the server certificate file contains the following:

a. Certificate chain starting with the server certificate which identifies the server and ending with the self-signed CA root certificate.

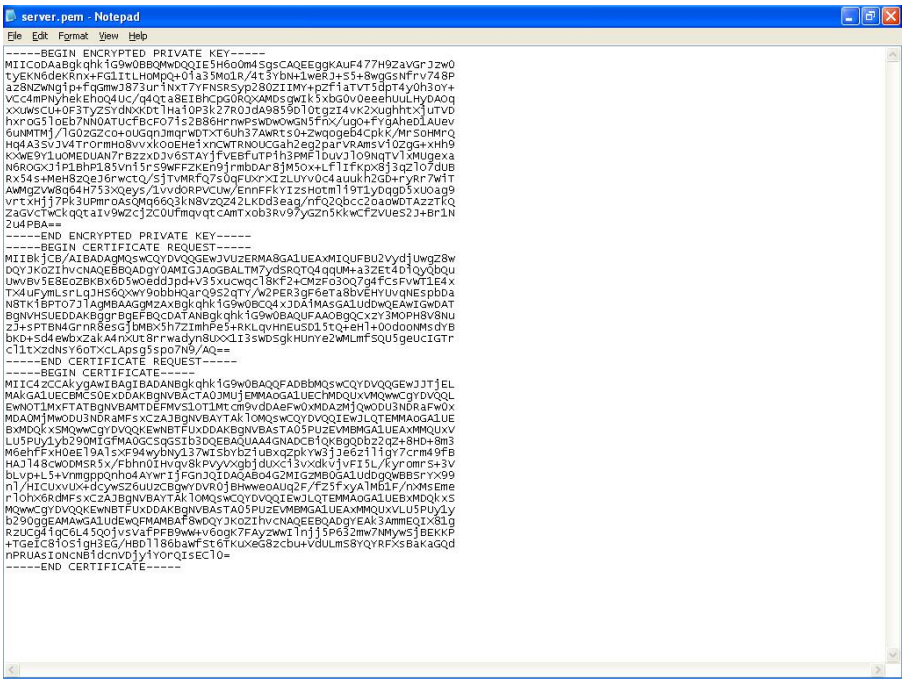
b. An encrypted version of the private key associated with the public key contained in the server certificate.

9 Using a text editor, such as Notepad, combine the private keys from the *Certificate Manager*, *server.cer*, and *ca.cer* in ..*AAA**run* directory. Save the file as *server.pem* in the *run* directory.

Note: Ensure that the file name is *server.pem* and not *server.pem.txt*.

Result: Figure 15-10 displays the combined certificates.

Figure 15-10 Combining certificates



Modify the *Private-Key-Password* attribute from the *security_properties* file in run directory. Ensure that this attribute is populated with password used for encrypting the server certificate private key in the 8950 AAA Certificate Manager.

A Machine authentication

Overview

The policies on the local machine need to be configured to allow machine authentication when using the EAP-PEAP-AD authentication protocol. Use this procedure to configure policies on the local machine.

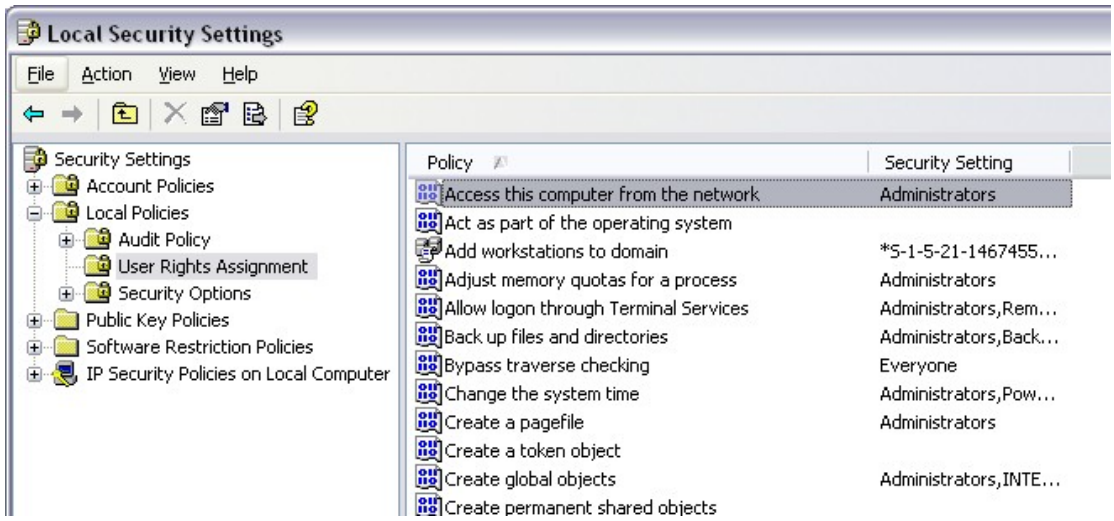
Procedure

1 On Windows, navigate to **Start** > **Control Panel** > **Administrative Tools** > **Local Security Policy**.

Result: The **Local Security Settings** window opens.

2 On the left navigation panel, expand **Local Policies** and select **User Rights Assignment**.

Figure 15-11 Local Security Settings



3 On the right panel, double-click **Access this computer from the network**.

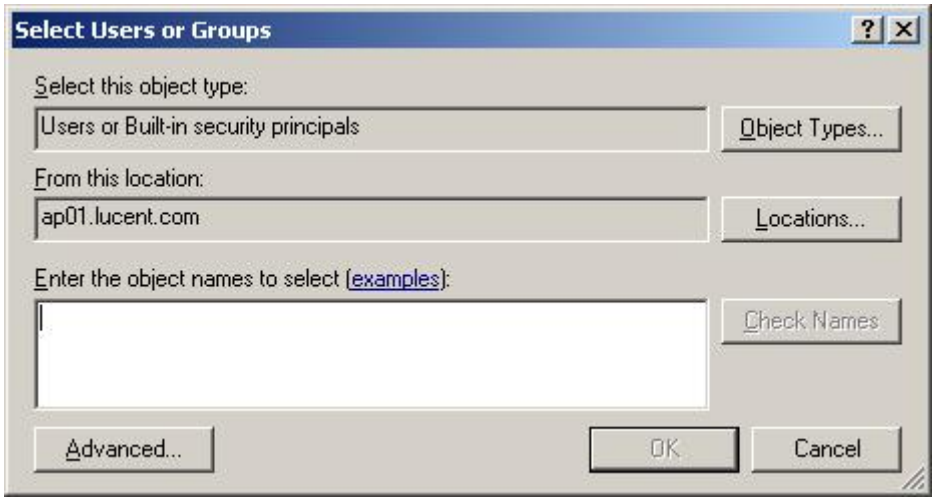
Figure 15-12 Access this computer from the network Properties

Access this computer from the network Properties
Local Security Setting
Explain This Setting
Access this computer from the network
Administrators
Add User or Group...
Remove
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Access this computer from the network. (Q823659)
OK
Cancel
Apply

4 Click **Add User or Group**.

Result: A dialog box to add or select users and groups opens.

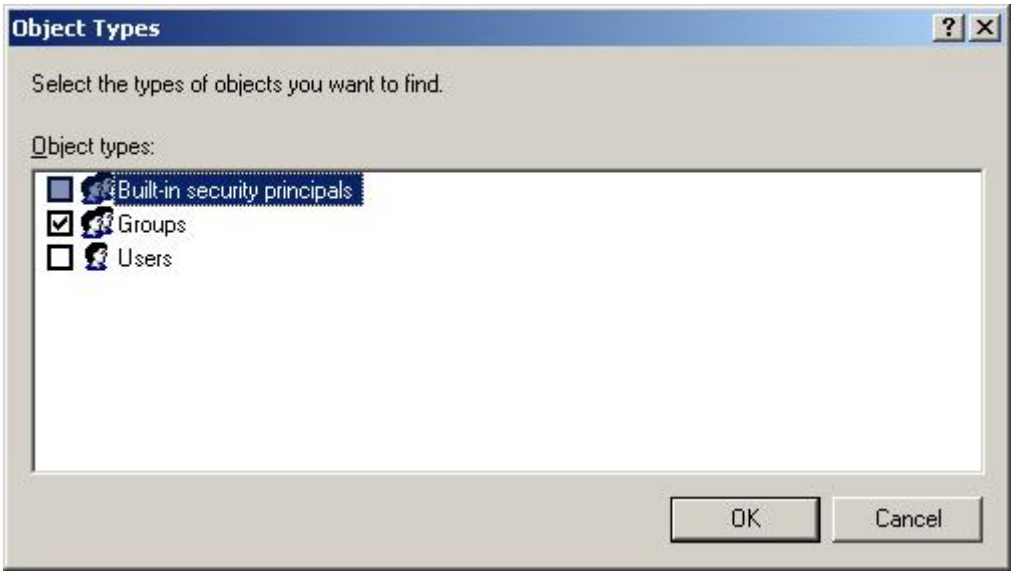
Figure 15-13 Select Users or Groups



5 Click **Object Types.**

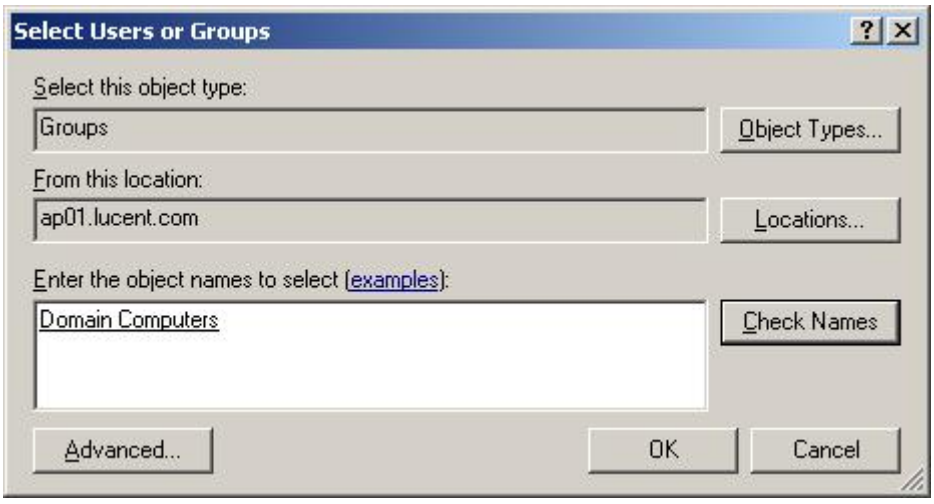
Result: The **Object Types** window opens.

Figure 15-14 Object Types



6 Check **Groups** and click **OK**.

Figure 15-15 Select Users or Groups



7 Enter **`Domain Computers`** in the text box and click **OK**.

Result: The policy window displays the updated content.

Figure 15-16 Local Security Setting

Access this computer from the network Properties
Local Security Setting
Explain This Setting
Access this computer from the network
Administrators
AP01\Domain Computers
Add User or Group...
Remove
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Access this computer from the network. (Q823659)
OK
Cancel
Apply

8 Click **Apply** and **OK** to save the changes. Accept all warnings.

9 Double-click **Act as part of operating system** in Figure 15-11.

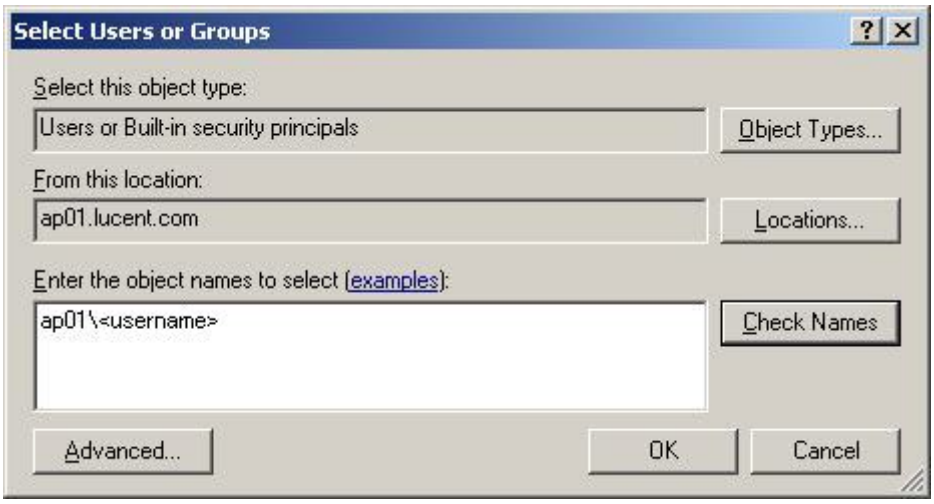
10 Click **Add User or Group**.

Result: A dialog box to add or select users and groups opens.

11 Enter the domain and the username.

Note: This user has the rights to call Windows APIs.

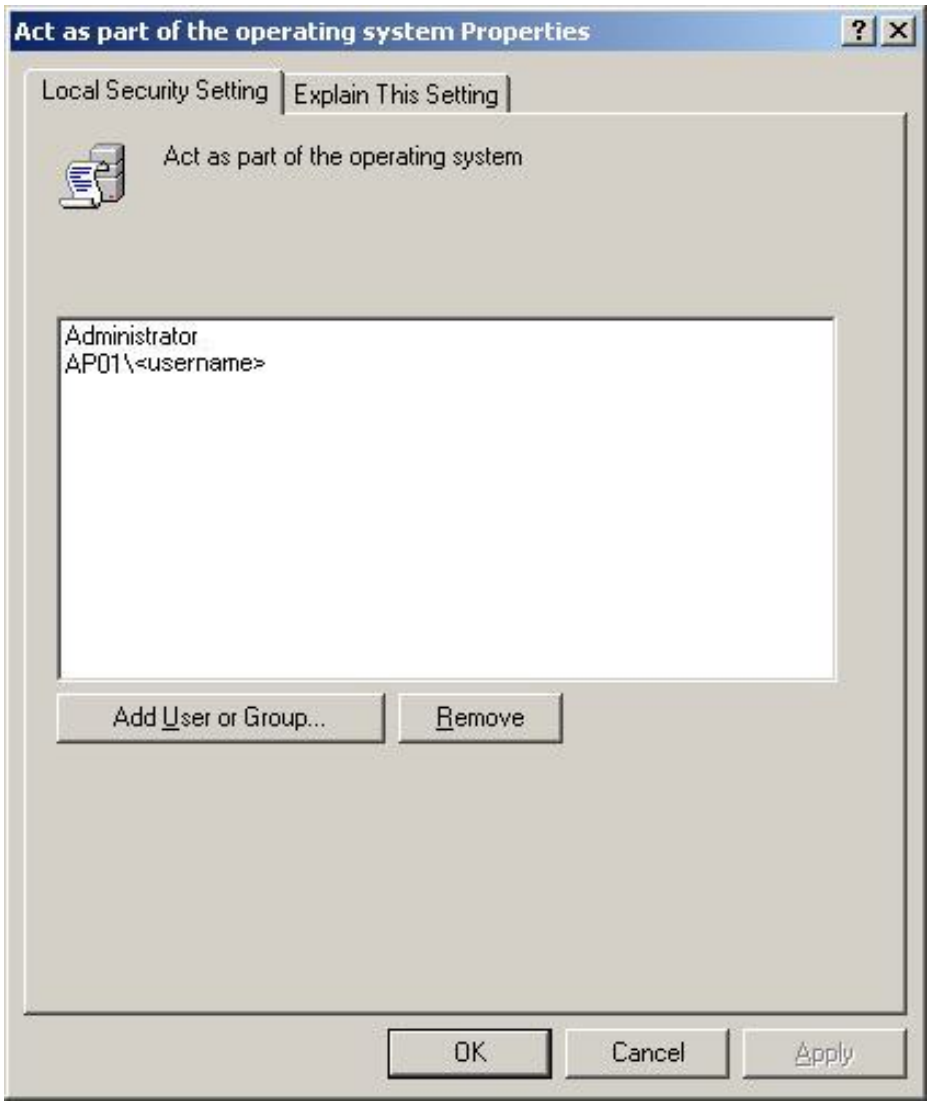
Figure 15-17 Select Users or Groups



12 Click **OK** to save the changes. Accept all warnings.

Result: The policies on the local machine are now configured to allow machine authentication.

Figure 15-18 Act as part of the operating system properties



Glossary

A

API
Application Programming Interface.

AAA
Authorizing, Authenticating and Accounting server

AD
Active Directory

C

CA
Certificate Authority

CLI
Command Line Interface

CIDR
Classless Inter-Domain Routing

CRL
Certificate Revocation List

E

EAP
Extensible Authentication Protocol

EAP-TLS
EAP-Transport Layer Security

EAP-TTLS
EAP - Tunneled Transport Layer Security

EAP-PEAP
EAP - Protected Extensible Authentication Protocol

EAP-MD5
EAP - Message-Digest algorithm 5

EAP-GTC
EAP - Generic Token Card

EBG
Enterprise Business Group

I

IANA
Internet Assigned Numbers Authority

L

LDAP
Lightweight Directory Access Protocol

M

MAC
Media Access Control

N

NAS
Network Access Server

R

RADIUS
Remote Authentication Dial In User Service

RMI
Remote Method Invocation

S

SAM
Security Access Manager

SMT
Server Management Tool

SNMP
Simple Network Management Protocol

T

TACACS
Terminal Access Controller Access-Control System

TLS
Transport Level Security

U

USS
Universal State Server

UPS
User Provisioning Tool

V

VLAN
Virtual Local Area Network

VSA
Vendor Specific Attributes

W

WLAN
Wireless Local Area Network